CyberAB.CMMC-CCP.v2026-07-01.q188

試験コード:	CMMC-CCP
試験名称:	Certified CMMC Professional (CCP) Exam
認定資格:	Cyber AB
無料問題数:	188
バージョン:	v2026-07-01
アクセス数:	105
ページビュー数:	1880
https://www.jpnpdf.com/CyberAB.CMMC-CCP.v2026-07-01.q188-mondaishu.html	

最新問題: **1**
CUIの信頼できるデータ分類が掲載されている資料はどれですか？
A. NARA
B. CMMC-AB
C. 国防総省請負業者に関するよくある質問
D. OSCのプライバシーポリシー
Answer: A (メーッセージを残す**)**
米国国立公文書館（NARA）は、米国連邦政府における機密指定されていない管理情報（CUI）プログラムを監督する権威ある機関です。NARAは、CUIのすべてのカテゴリー、サブカテゴリー、および関連する表示に関する決定的な情報源であるCUIレジストリを管理しています。このレジストリは、CUIの識別と取り扱いに関する包括的なガイダンスを提供し、連邦政府機関とその請負業者全体で標準化された慣行を保証します。
その他の選択肢は以下のとおりです。
* CMMC-AB :サイバーセキュリティ成熟度モデル認証認定機関は、CMMCプログラムの監督責任を負いますが、CUI分類の管理は行いません。
* 国防総省請負業者向け FAQ: これは国防総省の請負業者にガイダンスを提供する可能性がありますが、CUI データ分類に関する権威ある情報源ではありません。
* OSCのプライバシーポリシー：認証を求める組織の内部ポリシーは、その組織自身のデータ処理慣行に関するものであり、CUIの分類に関して権威を持つものではありません。
したがって、CUIデータ分類に関する信頼できる情報については、NARAのCUIレジストリが適切な情報源となります。

最新問題: **2**
CMMCモデル2.0は、どのような規格および規制要件に基づいていますか？
A. NIST SP 800-171およびNIST SP 800-172
B. DFARS、FIPS 100、およびNIST SP 800-171

C. DFARS、NIST、カーネギーメロン大学
D. DFARS、FIPS 100、NIST SP 800-171、およびカーネギーメロン大学
Answer: A (メーッセージを残す)
サイバーセキュリティ成熟度モデル認証（CMMC）2.0は、主に米国国立標準技術研究所（NIST）の2つの主要な特別刊行物に基づいています。
NIST SP 800-171 - 「非連邦システムおよび組織における管理対象非機密情報（CUI）の保護」NIST SP 800-172 - 「管理対象非機密情報を保護するための強化されたセキュリティ要件：NIST特別刊行物800-171の補足」参照と内訳：
NIST SP 800-171
この文書はCMMC 2.0の中核となる基盤であり、連邦政府以外のシステムにおける機密指定されていない管理情報（CUI）を保護するためのセキュリティ要件を定めています。
NIST SP 800-171 Rev. 2の110のセキュリティ管理項目は、CMMCレベル2に直接対応しています。
NIST SP 800-172
この補足資料には、高度な持続的脅威（APT）に直面する高価値のCUI（機密情報を扱う組織向けの強化されたセキュリティ要件が含まれています。
これらの強化された要件は、CMMC 2.0モデルにおけるレベル3に適用されます。
誤った選択肢を排除する：
B). DFARS、FIPS 100、およびNIST SP 800-171#不正解
DFARS 252.204-7012ではNIST SP 800-171への準拠が義務付けられているが、FIPS 100は関連するサイバーセキュリティ標準としては存在しない。
C). DFARS、NIST、カーネギーメロン大学#不正解
CMMCはDFARSおよびNISTに準拠していますが、カーネギーメロン大学によって開発されたものではなく、また同大学が直接影響を与えたものでもありません。
D). DFARS、FIPS 100、NIST SP 800-171、およびカーネギーメロン大学#誤り。FIPS 100は関係ありませんし、カーネギーメロン大学はCMMCフレームワークの定義エンティティではありません。
回答を裏付ける公式CMMC 2.0参照資料：
CMMC 2.0 スコープガイド（2023年）は、CMMCレベル2がNIST SP 800-171に完全に基づいていることを確認しています。
CMMC 2.0 レベル 3 ドラフト文書では、強化されたセキュリティ要件に関して、NIST SP 800-172 を明示的に参照しています。
国防総省暫定規則（DFARS 252.204-7021）は、組織がCUI保護に関してNIST SP 800-171を満たすことを義務付けています。
最終結論：
CMMC 2.0モデルはNIST SP 800-171とNIST SP 800-172のみに基づいて作成されているため、回答Aが唯一の正解です。

最新問題: 3

レベル2評価の結果パッケージが提出されます。CMMC評価結果の最終報告書には、何を含める必要がありますか？
A. 各実践または管理に対する肯定
B. 失敗した各実践に対する文書化された根拠
C. 失敗した実践例それぞれに対する改善提案
D. 相互主義モデルによるギャップまたはデルタは、満たされたと記録されます。
Answer: (解答を表示する**)**
CMMCレベル2最終報告書の要件を理解する
CMMCレベル2評価の場合、最終CMMC評価結果報告書には以下を含める必要があります。
各診療所の評価結果
各診療所の最終評価（達成または未達成）
「未達成」と評価された各項目について、詳細な根拠を示す。
B. 各失敗事例に対する文書化された根拠」が正しい理由は？
CMMC評価プロセス（CAP）ガイドでは、ある基準が満たされていないと判断された場合、評価者はその基準を満たしていない理由を説明する根拠を提示しなければならないと規定されている。
この根拠は、OSCが是正が必要な事項を理解し、該当する場合は、その不備が行動計画およびマイルストーン（POA&M）によって対処可能かどうかを判断するのに役立ちます。
最終報告書は公式記録として機能し、結果報告書の一部として提出されなければなりません。
他の回答が間違っている理由とは？
A) 各実践または管理に対する肯定（誤り）
報告書には各診療行為に対する「完了／未完了」の評価が含まれていますが、承認は必須項目ではありません。
C) 各失敗例に対する改善案（誤り）
評価者は改善のための提言は行わず、調査結果と根拠のみを記録する。
提案を行うことは、CMMC-ABの専門職倫理規定に基づき、利益相反を生じさせることになります。
D) 相互主義モデルによるギャップやデルタは、満たされたと記録される（誤り）組織が相互主義（例FedRAMP、共同監視自主評価）を活用している場合でも、ギャップは文書化されなければならず、「満たされた」と自動的にマークされることはありません。結論 正解はBです。これは、最終CMMC評価結果レポートの必須要件であるため、失敗した各プラクティスの根拠を文書化する必要があります。
参考文献：
CMMC評価プロセス（CAP）ガイド
DFARS 252.204-7021

最新問題**: 4**

評価チームは、OSCの要請に基づき、レベル2の評価を実施しています。チームは、提供された証拠に基づいて診療行為の採点を開始しました。診療行為がMET（基準を満たしている）と評価されるかどうかを判断するために、評価チームに最低限求められることは何ですか？
A. すべての対照群について、3種類の証拠すべてが文書化されています。
B. ３種類の証拠のうち 1つを検討し、採用する。
C. 以下のいずれかを完了してください。2 つのアーティファクトを検査し、1 つの制御の満足のいくデモンストレーションを観察するか、OSC 担当者から 1 つの確認を受けます。
D. 以下のうち2つを完了する :1つのアーティファクトを検査する、1つの制御の満足のいくデモンストレーションを観察する、またはOSC職員から1つの確認を受ける。
Answer: (解答を表示する**)**
この質問は、CMMC評価チームがレベル2評価において、ある診療所をMETと評価するために必要な最低限の証拠要件に関するものです。
CMMCレベル2の評価は、NIST SP 800-171に準拠し、特に証拠収集と採点方法に関して、CMMC評価プロセス（CAP）ガイドv1.0に概説されている手順に従う必要があります。
#ステップ 1: CMMC 評価プロセス (CAP) ガイド v1.0 を参照します。CAP v1.0 - セクション 3.5.4: 証拠の評価とスコアリング 実践「MET 判定を行うには、評価チームは、成果物の検査、インタビュー (確認)、またはテスト (実証) のいずれかを通じて、少なくとも 2 種類の客観的証拠を収集し、裏付けなければなりません。」これは、以下の証拠のうち少なくとも 2 種類が必要であることを意味します。
* 調査（文書成果物）、
* 面接（担当者からの確認）
* テスト（実装のデモンストレーション）。
#ステップ2：評価される実践の公式最低基準を明確にするCAPは明確に次のように述べています。
「診療行為がMETと評価されるのは、EIT（診察、面接、検査）の3つの要素から少なくとも2種類の証拠が適切に収集され、評価された場合に限られる。」
* 証拠の種類は、例えば以下の2つの異なるカテゴリーから取得する必要があります。
* 遺物（調査）＋インタビューでの肯定（インタビュー）、
* 実演（テスト）＋面接（インタビュー）
* その他
この相互検証により、制御策が確実に実施され、文書化され、担当者に理解されていることが保証されます。これは、効果的なサイバーセキュリティの実装を評価する上での中核となる原則です。
#他の選択肢が間違っている理由A. すべてのコントロールについて、3 種類の証拠すべてが文書化されている#間違い: 3 種類すべて (EIT) を収集することで評価は強化されますが、最低限必要なのは 2 種類だけです。実践が MET と評価されるために、3 種類すべてを収集する必要はありません。

B: 3 種類の証拠のうちの 1 つから証拠を検討し、受け入れる#不正解:これは CAP が定める最低 2 種類の証拠の要件を満たしていません。単一の情報源からの証拠では、実践を MET と評価するには不十分です。
C: 次のいずれかを完了してください。2 つの遺物を調べる、1 つの実演を観察する、または 1 つの確認を受け取る#誤り: 2 つの遺物を調べても、これは証拠の種類 (調べる) の 1 つだけです。CAP では 2 種類の証拠が必要であり、同じ種類の証拠が 2 つ必要ではありません。
#Dが正解である理由D. 次の2つを完了する :1つのアーティファクトを検査する、1つのコントロールの満足のいくデモンストレーションを観察する、またはOSC職員から1つの確認を受ける。
これは、診療がMETであるかどうかを判断するために、2種類の異なる客観的証拠を収集するというCAPの要件を直接反映しています。
要点 :CMMCレベル2の実践をMETと評価するには、評価チームは、検査、インタビュー、テスト（IT）のカテゴリから少なくとも2種類の異なる証拠を収集する必要があります。
この要件は、CMMC評価プロセス（CAP）v1.0に明確に記載されています。

最新問題**: 5**
遠隔地のクライアントサイトで評価が実施されています。評価期間中、クライアントはセキュリティ施設内に専用の宿泊スペースを用意しており、そこには共有プリンターにアクセスできるデスクがあります。デスクに鍵がかからないことに気づいたため、施錠可能なキャビネットを要求しましたが、クライアントは用意できませんでした。一日の終わりに、クライアントは重要なネットワーク図の印刷物を提供しました。この図にはCUI（機密情報）が含まれていることが明確に示されています。この文書を保護するために、次に何をすべきでしょうか？
A. 夕方に一緒に復習しましょう。
B. 翌日に検討するため、机の上に置いておく。
C. 翌朝確認するために、鍵のかかっていない机の引き出しに入れておく。
D. 安全にシュレッダーにかける前に、携帯電話で写真を撮っておきましょう。
Answer: A (メーッセージを残す**)**
このシナリオでは、十分な物理的セキュリティ対策（具体的には、施錠されたキャビネットや引き出しがない）が欠如している環境において、機密指定されていない管理情報（CUI）を保護することが主な懸念事項となります。
CMMC評価プロセス（CAP）およびNIST SP 800-171（特に物理的保護（PE）ファミリー）によれば、CUIは常に不正アクセスから保護されなければならない。
評価者の責任 :CMMCプロフェッショナル（CCPおよびCCA）は、CMMC専門職行動規範およびC3PAOの内部セキュリティプロトコルに従い、認証を求める組織（OSC）から提供されるCUIが安全に取り扱われることを保証する義務があります。

物理的保護（PE.L2-3.10.1 および PE.L2-3.10.2）これらの手順では、組織がシステムおよび機器への物理的アクセスを許可されたユーザーに限定し、物理的な施設を保護することが求められます。
「ホテルスペース」では、CUIを夜間安全に保管するための施錠可能な容器（キャビネットなど）が提供されていないため、CUIを施錠されていない引き出し（オプションC）や机の上（オプションB）に放置することは、CUIの取り扱いに関する要件に違反し、セキュリティ上のリスクとなります。
オプションAが最適な「次のステップ」である理由：現場に安全な保管場所がない場合、評価者は機密情報（CUI）を確実に管理する必要があります。評価者が管理下に置くことができる安全な場所（評価者のホテルの部屋や本人など）に文書を持ち込むことが、夜間に顧客サイトで清掃員やその他の許可されていない人員による不正アクセスを防ぐ唯一の有効な方法です。
他の選択肢が間違っている理由：
オプションBとC：どちらも、安全性の低い共有環境において、CUIを不正アクセスから保護することができません。
選択肢D：個人用携帯電話でCUIの写真を撮ることは、重大なセキュリティ違反（情報漏洩）です。なぜなら、個人用デバイスは通常、CUIを保存または処理することが許可されていないからです。
参考資料：
CMMC評価プロセス（CAP）v1.0：「CUIおよび専有情報に対する評価者の責任」に関するセクション。NIST SP 800-171 Rev 2：物理的保護（PE）ファミリー（3.10.1、3.10.2）。
国防総省指令5200.48「管理対象非機密情報（CUI）」では、CUIは権限のある個人の直接の管理下にない場合、少なくとも1つの物理的な障壁によって保護されなければならないと規定されています。

最新問題: 6
While conducting a CMMC Level 2 Assessment, a CCP is reviewing an OSC's personnel security process.
They have a policy that describes screening individuals prior to authorizing access to CUI, but it does not mention what organizations should be looking for in an individual. There is no link to a process or procedural document. What should the OSC evaluate when screening individuals prior to accessing CUI?
A. They are trusted and well liked
B. They are a hard and loyal worker
C. Their conduct, integrity, and loyalty
D. Their functionality, reliability, and ability to adapt
Answer: C (メーッセージを残す)
Under NIST SP 800-171, Personnel Security (PS) family, requirement PS.L2-3.9.1, organizations must screen individuals prior to granting access to CUI. The screening is

intended to evaluate conduct, integrity, and loyalty to ensure that individuals can be trusted with sensitive information.
Supporting Extracts from Official Content:
NIST SP 800-171 Rev. 2, PS.L2-3.9.1: "Screen individuals prior to authorizing access to organizational systems containing CUI... Screening is intended to assess an individual's conduct, integrity, judgment, loyalty, and reliability." CMMC Level 2 Assessment Guide (Personnel Security practices): confirms that screening covers conduct, integrity, and loyalty.
Why Option C is Correct:
The key attributes explicitly listed are conduct, integrity, and loyalty.
Options A and B describe subjective or informal measures, not compliance criteria.
Option D uses terms not aligned with the official requirement.
References (Official CMMC v2.0 Content):
NIST SP 800-171 Rev. 2, Personnel Security controls.
CMMC Assessment Guide, Level 2 - PS.L2-3.9.1.

最新問題**: 7**
クライアントが、CUI（機密情報に該当すると合理的に判断されるデータを保存、処理、または送信するために、外部のクラウドベースサービスを利用しています。DFARS条項252.204-7012によれば、そのクラウドプロバイダーはどのような確立されたセキュリティ要件を満たさなければなりませんか？
A. FedRAMP High
B. FedRAMP Low
C. FedRAMP 中程度
D. FedRAMP Secure
Answer: C (メーッセージを残す**)**

最新問題**: 8**
主任評価者および評価チームのメンバーは、必要に応じて、評価最終勧告結果概要から何日以内に、(OSCの更新されたPOA&Mと付随する証拠または予定されている収集物の正確性と妥当性をレビューする必要がありますか?
A. 90日間
B. 180日
C. 270日
D. 360日
Answer: (解答を表示する**)**
CMMC 2.0 の評価プロセスでは、評価最終推奨事項概要の後、主任評価者と評価チームのメンバーは、認証を求める組織 (OSC) の更新された行動計画とマイルストーン (POA&M) および付随する証拠または予定されている収集物の正確性と妥当性を 180 日以内に確認する必要があります。

関連するCMMC 2.0の参照資料：
CMMC評価プロセス（CAP）では、組織は最初の評価後、特定された不備に対処するために最大180日間の猶予が与えられると規定されています。
この期間中、OSCは遵守を証明するための追加証拠を添えて、POA&Mを更新することができる。
正解が180日（B）である理由は？
A) 90日間 # 不正解
CMMC CAPでは、POA&Mの更新に90日間の制限は設けられておらず、180日間が標準的な期間となっています。
B) 180日 # 正解
CMMC評価プロセスのガイドラインに従い、主任評価者とチームは180日以内に更新内容を確認する必要があります。
C). 270日 # 不正解
CMMCの公式文書には、270日間のレビュー期間に関する記述は一切ありません。
D). 360日 # 不正解
法令遵守を維持するためには、このプロセスは360日よりもはるかに早く完了しなければならない。
この回答を裏付けるCMMC 2.0の参考文献：
CMMC評価プロセス（CAP）文書
OSCがPOA&Mを更新し、審査のための証拠を提出するための180日間の期間を規定する。
CMMC 2.0 公式ガイドライン
組織には、再評価の前に不備を是正するために最大180日間の猶予が与えられることを規定している。

最新問題: **9**
DFARS条項252.204-7012は、どのような目的で必要とされるのですか？
A. FARパート12の手続きを使用する入札および契約
B. 市販品の調達のみを目的とする調達
C. 国防総省のすべての入札および契約
D. 市販品で、改造せずに市場で販売されているもの
Answer: C (メーッセージを残す**)**

最新問題: **10**
各診療科における評価方法の最終決定権は誰にあるのですか？
A. 中国共産党
B. osc
C. サイトマネージャー
D. 主任評価者
Answer: D (メーッセージを残す**)**

各プラクティスの評価方法は誰が決定するのですか？CMMCレベル2の評価では、主任評価者が各プラクティスを評価するために使用される評価方法を決定する最終的な権限を持ちます。
主任評価者の主な責任#CMMC評価プロセス（CAP）ガイドが遵守されていることを確認する。
面接、実演、文書レビューのいずれを使用して実務を評価するかを決定します。
#認定CMMCプロフェッショナル（CCP）およびその他の評価者に対し、証拠収集の方法論を指示する。
#適切な評価実施を保証するため、認定第三者評価機関（C3PAO）の下で業務を行います。
* CCP（オプションA）は評価を支援しますが、方法に関する最終決定は行いません。
* OSC（オプションB）は認証を求める組織であり、評価方法を管理する組織ではありません。
* サイトマネージャー（オプションC）は物流の調整を行うことはできますが、評価に関する決定権はありません。
「主任評価者」が正解である理由？回答選択肢の内訳
説明
正しい？
A: 中国共産党
#誤り - CCPassistsは評価方法を決定するものではありません。
B: OSC
#誤り - OSCは評価を受けている側であり、評価方法を決定する側ではありません。
C: サイトマネージャー
#誤り - サイトマネージャーは物流を担当しますが、評価方法を管理するわけではありません。
D：主任評価者
#正解 - 主任評価者が使用する評価方法について最終決定権を持ちます。
* CMMC評価プロセスガイド（CAP）-評価方法を決定する際の主任評価者の役割を定義します。
CMMC 2.0 ドキュメントからの公式参照最終検証と結論正解は D. 主任評価者です。主任評価者は評価方法論に対する最終的な決定権限を持っています。

最新問題: **11**
OSCが今後の評価のために証拠を提出しました。評価者はその証拠を審査し、CMMCの基準を満たすには不十分であると判断しました。評価者はどのような対応を取ることができますか？
A. CMMC-ABに通知する。
B. 評価をキャンセルする。
C. 評価を延期する。
D. C3PAOに連絡して指導を受けてください。

Answer: D (メーッセージを残す)
ステップ 1: 評価者の役割と責任の連鎖を理解するCMMC の評価中、評価者は C3PAO (認定第三者評価機関) によって組織されたチームの一員です。評価者が証拠が不十分または不適切であると判断した場合でも、評価を中止または延期する権限は独立してありません。
出典 :CMMC評価プロセス（CAP）v1.0 - セクション3.5.4および3.5.6
「評価チームが証拠の十分性または適切性に欠陥があると判断した場合、主任評価者およびC3PAOと協力して適切な対応策を決定しなければならない。」
* C3PAOは、評価ライフサイクル全体を監督する責任を負います。
* 証拠が不十分な場合、評価者は組織内（すなわち、主任評価者またはC3PAOの担当者）で以下の担当者に報告する必要があります。
* OSCに説明を求める、
* 追加の証拠を要求できるかどうかを判断する。
* 評価スケジュールを継続するか、一時停止するか、または変更するかを決定する。
#ステップ2 :C3PAOに連絡することが正しい行動である理由
* A. CMMC-ABに通知する# 誤り。サイバーAB（旧CMMC-AB）は、評価の運用面には関与していません。日々の評価決定を管理していません。
* B. 評価の取り消し# 誤り。評価者は一方的に評価を取り消すことはできません。C3PAOのみが、関係者全員と協議の上で、そのような措置を取ることができます。
* C. 評価を延期する# 間違いです。延期はロジスティクス上の決定であり、個々の評価者ではなく、C3PAO を通じて管理する必要があります。
#他の選択肢が間違っている理由
評価者がOSCから提出された証拠がCMMCの要件を満たすのに不十分または不適切であると判断した場合、適切な対応策はC3PAOに相談することです。C3PAOはガイダンスを提供したり、適切な次のステップを調整したりします。

最新問題: **12**
国防総省の請負業者は、機密情報漏洩をどの政府機関に報告する義務がありますか？
A. FBI
B. 奈良
C. 国防総省サイバー犯罪センター
D. 国防次官（情報安全保障担当）
Answer: C (メーッセージを残す)
国防総省の請負業者は、CUI の侵害を誰に報告するのでしょうか? DFARS 252.204-7012 に従って、管理された非機密情報 (CUI) を扱うすべての国防総省の請負業者は、サイバーインシデントを国防総省サイバー犯罪センター (DC3) に報告する必要があります。
主な報告要件#CUIに関わるサイバーインシデントは、72時間以内にDC3に報告する必要があります。

#報告書は国防総省のサイバーインシデント報告ポータルを通じて提出する必要があります。
#請負業者は、将来の捜査に備えて法医学的証拠を保存しなければならない。
* FBI（オプションA）は犯罪捜査を担当しますが、国防総省の請負業者はサイバーインシデントをDC3に報告する必要があります。
* NARA（オプションB）はCUIレジストリを監督しますが、情報漏洩の報告については責任を負いません。
* 国防次官（情報安全保障担当）（オプションD）は、情報活動を担当し、事件報告は担当しません。
「DoD サイバー犯罪センター」が正解である理由。回答選択肢の内訳オプションの説明正解ですか？
A: FBI
#誤り - FBIは刑事事件を扱い、CUI漏洩の報告は扱いません。
B: NARA
#誤り - NARAはCUIレジストリを管理していますが、情報漏洩の処理は行っていません。
C: 国防総省サイバー犯罪センター
#正しい - DFARS 252.204-7012 によると、CUI に関わるサイバーインシデントは DC3 に報告する必要があります。
D: 国防次官（情報安全保障担当）
#誤り - この部署ではサイバーインシデント報告は取り扱っておりません。
* DFARS 252.204-7012 - DoD の請負業者に CUI 関連のサイバー インシデントを DC3 に報告することを義務付けています。
* 国防総省サイバー犯罪センター（DC3）ウェブサイト - サイバーインシデント報告のための公式プラットフォーム。
CMMC 2.0 および DFARS 文書からの公式参照最終検証と結論正解は C です。DFARS 252.204-7012 に従って、国防総省サイバー犯罪センターは、すべての国防総省請負業者が CUI の侵害を 72 時間以内に DC3 に報告することを義務付けています。

最新問題: **13**
レベル1の自己評価において、請負業者がFCIの基本的な安全対策要件を満たしていることを義務付けている規定または条項はどれですか？
A. FAR 52.204-21
B. 22CFR 120-130
C. DFARS 252.204-7011
D. DFARS 252.204-7021
Answer: A (メーッセージを残す**)**
1. CMMCレベル1におけるFCIの基本的な保護要件の理解 連邦契約情報（FCI）は、政府によって契約に基づいて提供または生成された情報で、一般公開を意図していないものと定義されます。

CMMCレベル1は、FAR 52.204-21（対象となる請負業者の情報システムの基本的な保護）に記載されている15のセキュリティ要件に準拠し、FCIの基本的な保護を確保するように設計されています。
FCIのみを扱う請負業者は、FAR 52.204-21で定められた安全対策要件に直接準拠するCMMCレベル1を満たす必要があります。
2. FAR 52.204-21とCMMCレベル1準拠におけるその役割
FAR 52.204-21は、FCIを保護するために請負業者が実施しなければならない基本的なサイバーセキュリティ管理を定めています。
15の基本的な安全対策要件は以下のとおりです。
情報へのアクセスを許可されたユーザーのみに制限する。
システムへのアクセスを許可する前に、ユーザーを識別し認証する。
送信されたFCIを不正な開示から保護する。
外部システムへの接続を監視および制御する。
境界保護およびサイバーセキュリティ対策の適用。
廃棄前に培地を消毒する。
セキュリティ設定を更新して脆弱性を低減する。
物理的なセキュリティ対策を提供する。
FCIを処理するシステムへの物理的なアクセスを制御する。
該当する場合は、多要素認証（MFA）を強制的に適用する。
ソフトウェアおよびハードウェアの脆弱性を修正する。
リムーバブルメディアの使用を制限する。
システム監査ログの作成と保持。
リスクベースのセキュリティ評価を実施する。
インシデント対応計画の策定。
これら15のプラクティスは、CMMCレベル1自己評価の基礎を形成し、請負業者がFCIの取り扱いに関する最低限のサイバーセキュリティ要件を満たしていることを保証します。
3. 他の選択肢が間違っている理由
B) 22 CFR 120-130:
これは、防衛関連の物品およびサービスの輸出を規制する国際武器取引規則（ITAR）を指しており、FCIの安全保障要件とは関係ありません。
C). DFARS 252.204-7011:
この条項は代替的な明細項目構造に関するものであり、サイバーセキュリティやFCIの保護には関係しません。
D). DFARS 252.204-7021:
この条項は CMMC 要件を強制しますが、基本的な保護管理を定義しません。CMMC への準拠を要求しますが、基礎要件 (FAR 52.204- から得られる) を規定しません。
レベル1の場合は21）。
4. 公式CMMC 2.0リファレンスおよび学習ガイドとの整合性

CMMC 2.0 モデルのドキュメントでは、レベル 1 は FAR 52.204-21 の 15 の実践に重点を置いていることが確認されています。
国防総省の公式CMMCレベル1評価ガイドでは、FAR 52.204-21を満たすことがレベル1自己評価に合格するための要件であると明記されています。
CMMC 2.0 スコープガイドでは、FCI のみを取り扱い、レベル 1 認証を申請する請負業者は、FAR 52.204-21 のセキュリティ管理策のみを実施する必要があることが明確にされています。
最終確認: 正解は A. FAR 52.204-21 です。これは FCI の基本的な保護を直接規定しており、CMMC 2.0 のレベル 1 自己評価の基礎となる要件です。

最新問題**: 14**
OSC（特別監視センター）が、メール本文に「CUI//SP-PRVCY//FED Only」と記載されたメールを受信した場合、この表記の意味を確認するには、どの組織のウェブサイトにアクセスすればよいでしょうか？
A. NARA
B. CMMC-AB
C. 国防総省請負業者向けFAQページ
D. DoD 239.7601 定義ページ
Answer: (解答を表示する**)**
「CUI//SP-PRVCY//FED Only」とはどういう意味ですか？
このメールには、特定のカテゴリと配布制限が定められた管理対象非機密情報（CUI）が含まれています。
CUI//SP-PRVCY//FED は以下のように分解されます。
CUI# 管理対象非機密情報指定番号。
SP-PRVCY#プライバシー情報のための指定カテゴリ（SPは「指定」を意味します）。
連邦政府専用# 連邦政府専用（請負業者や一般の方は使用できません）。
公式CUI登録簿を管理しているのは誰ですか？
米国国立公文書館（NARA）はCUIプログラムを監督し、公式のCUIレジストリ（https://www.archives.gov/cui）を維持管理しています。
CUIレジストリは、「SP-PRVCY」や「FED Only」などの配布制御を含む、すべてのCUIラベルの定義、マーキングガイダンス、カテゴリを提供します。NARAが正解である理由 NARAは、CUIマーキングの定義と管理を担当する統括機関です。
CUI（機密情報）を取り扱う組織は、公式な表示解釈についてはNARA（米国国立公文書館）のCUI登録簿を参照する必要があります。
国防総省の請負業者およびその他の組織は、機密情報（CUI）の取り扱い、表示、および配布を行う際に、米国国立公文書館（NARA）のガイドラインを遵守しなければならない。
B) CMMC-AB - CMMC認定機関は認証評価を管理しますが、CUIマーキングを定義または解釈しません。

C) DoD 請負業者 FAQ ページ - DoD は一般請負業者向けのガイダンスを提供する場合がありますが、CUI の表示は NARA によって管理されており、FAQ ページではありません。
D). DoD 239.7601 定義ページ - これは一般的な国防総省の調達定義を参照していますが、CUI のカテゴリとマーキングは NARA の権限下にあります。
参考文献 :NARA CUIレジストリ（https://www.archives.gov/cui）
DoD CUI プログラム ガイダンス (DoD CIO サイト)
CMMC 2.0 レベル2 準拠要件（サイバーAB）
#最終回答 A. NARA

最新問題**: 15**
Which document is the BEST source for descriptions of each practice or process contained within the various CMMC domains?
A. CMMC Glossary
B. CMMC Appendices
C. CMMC Assessment Process
D. CMMC Assessment Guide Levels 1 and 2
Answer: D (メーッセージを残す)
Understanding the Best Source for CMMC Practice DescriptionsTheCMMC Assessment Guide (Levels 1 and
2)is theprimaryandmost authoritativedocument for detailed descriptions of each practice and process within the variousCMMC domains.
Step-by-Step Breakdown:#1. What is the CMMC Assessment Guide?
TheCMMC Assessment Guideprovides detailed explanations of:
EachCMMC practicewithin its respectivedomain.
Theassessment objectivesfor verifying implementation.
Examples ofevidence requiredto demonstrate compliance.
CMMC 2.0 includes two levels:
Level 1: 17 basic cybersecurity practices.
Level 2: 110 practices aligned withNIST SP 800-171.
TheAssessment Guidedefines howassessorsevaluate compliance.
#2. Why the Other Answer Choices Are Incorrect:
(A) CMMC Glossary#
TheGlossaryprovidesdefinitions of termsused in CMMC but does not describe specific practices in detail.
(B) CMMC Appendices#
Appendicesinclude supplementary information likereferences and scoping guidance, but they do not provide full descriptions of practices.
(C) CMMC Assessment Process#
TheAssessment Process Guideexplainshowassessments are conducted, but it doesnot describe each practicein detail.

Final Validation from CMMC Documentation:TheCMMC Assessment Guide (Levels 1 and 2)is theofficialsource for descriptions of eachCMMC practice and process, making it thebest referencefor understanding compliance requirements.

最新問題: **16**
収集した証拠が十分かどうかを判断するための基準として適切でない記述はどれですか？
A. 証拠はサンプリングされた組織を対象としています
B. ISO認証を受けている場合は、証拠は不要です。
C. 証拠は評価のモデル範囲を網羅している（目標CMMCレベル）
D. 証拠は、証拠収集アプローチにおけるサンプリングされた組織に対応する。
Answer: B (メーッセージを残す**)**
CMMC評価プロセス（CAP）では、十分な証拠が以下の要件を満たす必要があります。
サンプリングされた組織をカバーする、
評価の定義されたモデル範囲（目標CMMCレベル）を網羅し、証拠収集方法に準拠していること。
組織がISOなどの他の認証を取得している場合でも、証拠は常に必要です。外部認証はCMMCの証拠要件に取って代わることはできません。したがって、「ISO認証を取得している場合は証拠は不要」という主張は妥当ではありません。
参考資料：
CMMC評価プロセス（CAP）、v1.0

有効な **CMMC-CCP** 問題集は GoShiken.com が提供された合格しやすい CMMC-CCP 試験問題集！ GoShiken.com が最新の **CMMC-CCP** 試験問題集を提供しています。GoShiken.com CMMC-CCP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CMMC-CCP 問題集をゲットする人はこちら: https://www.goshiken.com/Cyber-AB/CMMC-CCP-mondaishu.html (**23030%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **17**
評価範囲を定める際、評価者は評価範囲が何を網羅しているかを確認すべきでしょうか？
A. 事業分野を問わず、組織に関連するすべての事業体
B. FCI/CUIを処理、保存、送信するかどうかにかかわらず、すべての資産
C. FCI/CUIの処理、保管、送信を行うすべての資産、およびセキュリティ保護資産
D. 事業計画書に記載されているすべての資産
Answer: C (メーッセージを残す**)**

最新問題: **18**

レベル2評価の際、OSCは、非ローカルのリモートメンテナンスセッションで多要素認証を使用していることを証明する文書を提出しました。OSCは、レベル2認証の要件を満たしていると考えています。メンテナンス要件を完全に満たすために、OSCは他にどのような対策を講じるべきでしょうか？

A. メンテナンスが完了したら、非ローカルメンテナンスセッションの接続を終了する必要があります。

B. メンテナンスが適切に実施されるよう、非ローカルメンテナンスセッションの接続数は無制限にする必要があります。

C. 地元以外のメンテナンス担当者は、制限によって対応時間が遅くなると不満を述べており、制限は撤廃されるべきだと主張している。

D. メンテナンスポリシーでは、非ローカルメンテナンスセッションには多要素認証を少なくとも2つの要素で適用する必要があると規定されています。

Answer: A (メーッセージを残す)

NIST SP 800-171 の要件に準拠した CMMC 2.0 レベル 2 では、非ローカル保守セッションに対する堅牢な制御を維持することが不可欠です。多要素認証 (MFA) は安全なアクセスに必要な保護策ですが、制御 3.3.5 で概説されている保守要件を完全に満たすためには、追加の対策を実施する必要があります。

非現地メンテナンスの主な要件：

非ローカルメンテナンスセッションの終了:

攻撃対象領域を縮小し、不正アクセスを防止するため、メンテナンス作業完了後、非ローカルのメンテナンス接続は直ちに切断する必要があります。これは、脅威アクターによって悪用される可能性のある、リモートセッションの長期化に伴うリスクを軽減するための直接的な要件です。

参考資料：NIST SP 800-171、コントロール3.3.5には、「リモートメンテナンスは管理された方法で実施し、使用後は直ちに接続を無効にすること」と記載されています。多要素認証（MFA）：

OSC（運用保守センター）は、非ローカルのリモート保守セッションに対してMFA（多要素認証）を実装する必要があります。MFAには、少なくとも2つの要素（例えば、知っていること、持っているもの、または自分自身であること）を含める必要があります。

OSCによるMFAの利用は要件の一部を満たすものの、適切な終了手順が整備されていない限り、完全な制御とは言えません。

方針および手順の遵守：

OSCは保守ポリシーを文書化し、保守後に接続を終了させる必要性を反映させる必要がある。ポリシーには、安全な非ローカル保守手順を確保するための役割、責任、および手順を明記する必要がある。

誤った選択肢：

B) 無制限の接続: 無制限の非ローカルメンテナンスセッションを許可することは、重大なセキュリティリスクであり、最小権限の原則に違反します。

C) 制限の撤廃：便宜のために制限を撤廃することは、コンプライアンスとセキュリティを直接的に損なう。
D) 多要素認証の詳細: MFA は必要ですが、質問では OSC が既にそれを使用していると述べられています。
セッションの終了が、欠けている要件です。
結論：
メンテナンス完了後に非ローカルメンテナンスセッションを終了するという要件（オプションA）は、CMMC 2.0レベル2およびNIST SP 800-171、コントロール3.3.5への準拠に不可欠です。これにより、非ローカルメンテナンス活動が不正アクセスや潜在的な脆弱性から保護されることが保証されます。

最新問題: **19**
評価手順は、評価目標、評価方法、評価対象から構成されます。次のうち、評価目標の一部となる記述はどれですか？
A. 仕様と仕組み
B. 試験、面接、テスト
C. 実践に関する決定声明
D. 指定された条件下で評価対象を運動させる
Answer: C (メーッセージを残す**)**
CMMC評価手順の理解CMMC評価手順は以下で構成されます。
* 評価目標 - 評価対象と期待される結果を定義します。
* 評価方法 - 評価がどのように実施されるかを指定します（例：試験、面接、テスト）。
* 評価対象 - 政策、システム、人物など、評価対象となるものを特定します。
* 評価目標には、CMMCの各セキュリティ対策について期待される結果を説明する決定事項が含まれます。
* これらの記述は、文書化された証拠と評価結果に基づいて、ある実践が適切に実施されているかどうかを定義するものです。
* CMMC評価プロセス（CAP）ガイドおよびNIST SP 800-171Aでは、各プラクティスには評価の決定を導く決定ステートメントがあることが規定されています。
* A. 仕様とメカニズム#不正解
* これらは評価対象に属し、評価対象となるシステム、ポリシー、およびメカニズムを指します。
* B. 試験、面接、テスト#不正解
* これらは評価方法であり、評価者がコンプライアンスをどのように検証するか（例えば、面接やテストなど）を説明するものです。
* D. 指定された条件下で評価対象を運動させる#不正解
※これは評価テストに関するものであり、評価目標ではなく評価方法です。
* CMMC評価プロセス（CAP）ガイド - 評価目標の中核として決定事項を説明しています。

* NIST SP 800-171A - セキュリティ管理策を評価する上での重要な要素として、判定ステートメントを定義しています。
正解が「C」である理由。他の選択肢ではない理由。関連するCMMC 2.0の参照。最終的な正当化:評価目標には、プラクティスが適切に実施されているかどうかを説明する決定ステートメントが含まれているため、正解はCです。

最新問題: **20**
CMMCモデルにおいて、レベル2にはいくつのプラクティスが含まれていますか？
A. 17の実践
B. 72の実践
C. 110の実践例
D. 180の練習
Answer: C (メーッセージを残す**)**
* CMMCレベル2は、110のセキュリティ管理策（実践）で構成されるNIST SP 800-171に準拠するように設計されています。
* これは、NIST SP 800-171に記載されている110のプラクティスすべてがCMMCレベル2認証に必要であることを意味します。
CMMCレベル2にはいくつのプラクティスが含まれていますか？CMMC 2.0のプラクティスの内訳 CMMCレベル プラクティスの数 レベル1
17の実践事項（基本的なサイバー衛生）
レベル2
110の実践例（NIST SP 800-171に準拠）
レベル3
まだ確定していないが、110を超える見込み
CMMCレベル2ではNIST SP 800-171のすべての110のプラクティスが義務付けられているため、正解はCです。110のプラクティス。
* A. 17のプラクティス#誤り。17のプラクティスはCMMCレベル1にのみ適用され、レベル2には適用されません。
* B. 72 の実践#誤り。72 の実践を含む CMMC レベルはありません。
* D. 180の実践#間違いです。CMMCレベル2では110の実践のみが必要であり、180ではありません。
他の回答が間違っている理由
* CMMC 2.0 モデル - レベル 2 には NIST SP 800-171 に準拠した 110 のプラクティスが含まれていることを確認します。
* NIST SP 800-171 Rev. 2 - 管理対象非機密情報 (CUI) の取り扱いに必要な 110 のセキュリティ管理策の概要を示します。
CMMC公式資料によると、公式のCMMCガイダンスに従って、オプションC（110のプラクティス）が正解です。

最新問題: **21**

調査結果の検証は反復的なプロセスであり、通常は評価プロセス全体を通してデイリーチェックポイントで実施されます。検証活動として、予備的な調査結果が重要なのはなぜでしょうか？

A. OSCがコメントしたり、追加の証拠を提出したりすることを可能にします。

B. OSCが評価で「MET」と判定されるか「NOT MET」と判定されるかを決定します。

C. 評価チームの調査結果が正しいことを確認し、変更できないことを示します。

D. CMMCの実践と管理に関する評価チームの理解を裏付けるものです。

Answer: A (メーッセージを残す**)**

1. CMMC評価における調査結果の妥当性検証の理解

調査結果の検証はCMMC評価プロセスの重要な部分であり、評価チームが行った観察結果および予備的な結論が正確かつ公平であり、完全な証拠に基づいていることを保証するものです。

このプロセスは、日々のチェックポイントで繰り返し行われ、認証を求める組織（OSC）の全体的なコンプライアンス状況を判断する上で不可欠です。

2. 評価プロセスにおける予備調査結果の役割

予備調査結果は最終的なものではなく、透明性、正確性、公平性を確保するための仕組みである。

これらの研究結果は、いくつかの重要な目的を果たすものである。

OSCの意見提供と説明を可能にする：OSCは、評価チームが特定した不備に対処する可能性のある追加の証拠を検討し、提供する機会を得ます。

誤解を防ぐ：OSCがコメントできるようにすることで、評価チームはOSCによるCMMCの実施状況に関する理解を深めたり、修正したりすることができる。

公正かつ情報に基づいた評価を支援する：評価チームは、達成（MET）または未達成（NOT MET）の最終決定を行う前に、関連するすべての証拠を検討したことを確認します。

協調的な評価プロセスを促進する：この検証活動は、評価者とOSC間のオープンなコミュニケーションを促進し、紛争や誤解を減らします。

3. 選択肢「A」が正解である理由

予備調査結果の主な目的は、最終決定が下される前に、OSCが意見を述べ、追加の証拠を提出できるようにすることです。

これは、CMMC評価プロセスのガイダンスに沿ったものであり、日々のチェックポイントと最終的な報告会を通じて、調査結果を繰り返し検証することを重視しています。

調査結果の検証により、OSCの回答や補足的な証拠が考慮されることが保証され、評価プロセスがより正確かつ公平になります。

4. 他の選択肢が間違っている理由

オプション

除外理由

B) これは、OSCが評価において「MET」と評価されるか「NOT MET」と評価されるかを決定します。

誤り：予備調査の結果は、最終評価を直接決定するものではありません。評価チームは、最終決定を下す前に、収集したすべての証拠を検討します。
C) 評価チームの調査結果が正しいことを確認し、変更できないことを示す。
誤り：予備段階では調査結果は確定的なものではありません。OSC（特別検察官）は、新たな証拠や補足的な証拠を提出することで、調査結果に異議を申し立てる機会があります。
D) これは、CMMCの実践と管理に関する評価チームの理解を裏付けるものです。
部分的に正しいが、最良の回答ではない：検証は理解を深めるのに役立つが、その主な機能はOSC入力を可能にすることであるため、オプションAが最も正確な選択肢となる。
5. この回答を裏付ける公式CMMC参照資料
CMMC評価プロセス（CAP）文書：
セクション 5.3 - 調査結果の検証: 「OSC には、予備評価結果を明確化または補足するための追加の証拠とコメントを提供する機会が与えられます。」セクション 5.4 - 日々のチェックポイント: 「評価チームは OSC と予備調査結果について話し合い、組織が懸念事項にリアルタイムで対処できるようにします。」CMMC 2.0 レベル 2 スコープ設定および評価ガイド:
評価プロセスには、最終決定が下される前にOSCとの継続的な対話が含まれることを確認する。
6. 結論
予備調査結果は、CMMC評価における重要な検証ステップであり、組織が追加の証拠を提出し、潜在的な誤解を解消する機会を保証します。この反復プロセスにより、CMMC要件への準拠を判断する際の正確性と公平性が向上します。したがって、正解は次のとおりです。
A) オンタリオ州検察庁（OSC）が意見を述べたり、追加の証拠を提出したりすることを可能にする。

最新問題: **22**
CMMCは「実践」をどのように定義していますか？
A. 定義されたCMMCの目標を達成するために実施される活動または複数の活動
B. 定められた方法で起こる一連の変化
C. ビジネス取引
D. 経験や訓練によって到達した状態
Answer: A (メーッセージを残す**)**

最新問題: **23**
CCP（認定コンサルティングプロバイダー）がOSC（オープンサービス企業）にコンサルティングサービスを提供しています。CCPはOSCのCMMCレベル2評価の準備を進めています。OSCはCCPに対し、CMMC評価範囲の決定責任者と、その評価範囲の妥当性を確認する責任者は誰かを尋ねました。CCPはどのように回答すべきでしょうか？
A. 「OSCがCMMC評価範囲を決定し、CCPがCMMC評価範囲を検証します。」
B. 「CMMC主任評価者がCMMC評価範囲を決定し、OSCがCMMC評価範囲を検証する。」

C. OSCがCMMC評価範囲を決定し、C3PAOがCMMC評価範囲を検証する。」
D. CMMC C3PAOがCMMC評価範囲を決定し、主任評価者がCMMC評価範囲を検証する。」
Answer: C (メーッセージを残す)

最新問題: **24**
CMMCのスコープは、CUIが存在する場所に焦点を当てたシステム、アプリケーション、サービスを含むCUI環境を対象としています。
A. 受信および転送。
B. 保存、処理、送信。
C. 入力、編集、操作、印刷、閲覧。
D. 電子媒体、システムコンポーネントのメモリ、および紙媒体に存在する。
Answer: B (メーッセージを残す)
CMMCレベル2のスコープガイドでは、CUI資産には、管理対象非機密情報（CUI）を保存、処理、または送信するシステム、アプリケーション、およびサービスが含まれると概説しています。これらは、認証取得を目指す組織（OSC）におけるCUIの取り扱いを定義する3つの主要機能です。
段階的な解説：#1. CMMCで定義されているCUI資産
保存場所：CUIはハードドライブ、クラウドストレージ、またはデータベースに保存されます。
処理済み：CUIは、アプリケーションやユーザーによって積極的に使用、変更、または分析されています。
送信：CUIは、電子メール、ファイル転送、またはネットワーク通信を介してシステム間で送信されます。
#2. 他の選択肢が間違っている理由：
（A）受領および転送#
CUIの受領と移転はCUIの取り扱いの一部ではあるが、CUI資産に関するすべての責任を完全に網羅するものではない。
（C）入力、編集、操作、印刷、閲覧#
これらは処理内の特定のアクションですが、CMMCのスコープ設定に必要なストレージや送信は含まれません。
（D）電子媒体、システムコンポーネントメモリ、紙媒体に存在する# CUIは電子形式と物理形式で存在できますが、CMMCのスコープは、CUIが物理的に存在する場所ではなく、CUIがどのようにアクティブに管理されるか（保存、処理、送信）に焦点を当てています。
CMMCレベル2スコープガイドでは、CUI資産はCUIの保存、処理、または送信における役割に基づいて分類されることが確認されています。
NIST SP 800-171もまた、これら3つの機能をCUI保護の重要な構成要素として定義している。
CMMCドキュメントに基づく最終検証：

最新問題: **25**
SI.L1-3.14.2 組織の情報システム内の適切な場所で悪意のあるコードからの保護を提供する」を評価する際、OSCのすべてのワークステーションとサーバーに悪意のあるコードからの保護のためのウイルス対策ソフトウェアがインストールされていることが確認されました。ウイルス対策ソフトウェア管理のための集中管理コンソールが設置されており、すべてのデバイスに最新のウイルス対策パターンが適用されていることが記録から示されています。
主任評価者が証拠に関して下すべき最善の判断とは何でしょうか？
A. 不十分であり、主任評価者はさらなる証拠を求めるべきである。
B. 不十分であり、監査結果は 未達成」と評価されます。
C. それで十分であり、主任評価者はさらなる証拠を求めるべきである。
D. 十分であり、監査結果はMETと評価できます。
Answer: D (メーッセージを残す**)**

最新問題: **26**
CMMC 2.0の一環として、レベル1自己評価への変更により 評価コストの削減」が実現し、レベル1（基礎のすべての企業が以下のことが可能になります。
A. 自己評価を実施する。
B. CMMC評価を辞退する。
C. 年間評価額は500ドルを超えない。
D. 国防総省から評価費用の払い戻しを受ける。
Answer: (解答を表示する**)**

最新問題: **27**
評価チームが、文書化され毎月チェックされている業務手順を審査しています。ログを確認したところ、その業務手順は四半期ごとにしか実施されていないことが判明しました。面談で、チームメンバーは業務手順は毎月実施しているが、文書化は四半期ごとだと説明しました。この状況で、業務手順の合格基準を満たすことができるでしょうか？
A. いいえ、作業は記載どおりには行われていません。
B. はい、手順は文書に記載されているとおりに実施されています。
C. いいえ、合格するには3つの評価方法すべてを満たす必要があります。
D. はい。面接プロセスは練習に合格するのに十分です。
Answer: A (メーッセージを残す**)**
CMMC評価要件の理解
CMMC評価では、セキュリティ対策への準拠を確認するために3つの評価方法を使用します。
調査する - 文書、ポリシー、ログ、または記録を確認する。
インタビュー：担当者と面談し、理解度と実行状況を確認する。

テスト：技術的または運用上の手段を用いて、その手順が実行されていることを検証すること。
提示されたシナリオにおける評価結果
練習は毎月実施されていると記録されているが、ログには四半期ごとに実施されていることが示されている。
インタビューでは月1回実施されていると示唆されているが、文書ではこの主張を裏付けていない。
組織が実践に失敗する理由
回答A（不正解）：作業行われているが、文書化が不十分なため、失敗は実行漏れだけが原因ではない。
回答B（不正解）：記録された頻度がログの証拠と一致しないため、手順は完全に記録された通りに行われていません。
正解はCです。CMMCでは、3つの評価方法（検査、インタビュー、テスト）すべてが一致している必要があります。ログに記載されている頻度と矛盾するため、この方法は準拠していません。
回答D（不正解）：インタビューの回答だけでは不十分です。CMMC-CAPガイドとNIST SP 800-
171ログ（調査）と技術的検証（テスト）による裏付けが必要です。
結論
正解はCです。組織が実務に合格するには、3つの評価方法すべてにおいて証拠を提出する必要があります。
CMMC評価プロセス（CAP）ガイド - Cyber AB
NIST SP 800-171A - CUIのセキュリティ要件の評価
DoD CMMC 2.0 スコープ設定および評価ガイド

最新問題: **28**
SI.L2-3.14.6「通信に対する攻撃の監視」を評価する際、CCAは侵入検知システムの責任者にインタビューを行い、組織システムの監視に関する関連ポリシーと手順を検証します。CCAが十分な証拠を収集するために次に実行できる可能性のある手順は何でしょうか？
A. 侵入テストを実施する
B. 侵入検知システムのサプライヤーにインタビューする。
C. 既知の悪意のあるコードをアップロードし、システムの反応を観察します。
D. 侵入検知および防御システムに関する追加のガイダンスを得るために、IDS または IPS プラクティスの構成に関する主要な参照を確認するために、成果物をレビューします。
Answer: D (メーッセージを残す**)**
SI.L2-3.14.6の理解：攻撃に対する通信の監視NIST SPの実践SI.L2-3.14.6
800-171（CMMCレベル2に準拠）では、組織は攻撃の兆候がないか組織内の通信を監視することが求められます。これには通常、以下が含まれます。
#侵入検知システム（IDS）と侵入防御システム（IPS）

#ログ分析とネットワーク監視
#検出された脅威に対するインシデント対応計画
CMMCレベル2評価の一環として、認定CMMC評価者（CCA）は、OSC（認証取得を目指す組織）が監視機能を適切に実装し、文書化していることを確認する必要があります。
* CCAは、コンプライアンスを判断するために十分な客観的証拠を収集しなければならない。
* システム構成、IDS/IPSログ、セキュリティポリシーなどの成果物をレビューすることで、侵入検知が適切に実装されていることを検証できます。
* 設定内容は、攻撃監視が効果的に実施されているかどうかを直接的に示す証拠となる。
「IDSまたはIPSの設定に関する重要な参照を確認するために、成果物をレビューする」が正しいのはなぜですか？
回答選択肢の内訳
説明
正しい？
A：侵入テストを実施する
#誤り - 侵入テストはCMMCレベル2の評価には必要なく、評価者の責任範囲外です。
B：侵入検知システムの供給業者にインタビューする。
#誤り - サプライヤーはコンプライアンスを判断しません。評価者はOSCの実施状況に関する証拠を必要とします。
C：既知の悪意のあるコードをアップロードし、システムの反応を観察します。
#誤り - これは侵襲的な検査であり、CMMC評価の一部ではありません。
D: 侵入検知および防御システムに関する追加のガイダンスを得るために、IDSまたはIPSの実践における構成に関する重要な参照事項を確認するために、成果物をレビューします。
#正解 - システム成果物をレビューすることで、SI.L2-3.14.6への準拠の直接的な証拠が得られます。
* NIST SP 800-171 SI.L2-3.14.6 - 攻撃の兆候を監視するために通信を監視する必要がある。
* CMMC評価プロセスガイド（CAP）- 成果物レビューを必須の評価方法として説明しています。
CMMC 2.0 および NIST SP 800-171 ドキュメントからの公式参照最終検証と結論正解は D です。侵入検知および防御システムに関する追加のガイダンスについては、IDS または IPS プラクティスの構成に関する主要な参照を確認するためにアーティファクトを確認します。
これは、CMMC 2.0 レベル 2 の評価要件および SI.L2-3.14.6 準拠検証に準拠しています。

最新問題: **29**
請負業者は、セキュリティポリシー、システム構成ファイル、監査ログを中央ファイルリポジトリに保存し、後で確認します。CMMCの用語によれば、ファイルリポジトリは次の目的で使用されます。

A. CUIを送信します。
B. CUIを保護する。
C. CUIを生成する
D. CUIを保存します。
Answer: D (メーッセージを残す)

最新問題**: 30**
How does the CMMC define a practice?
A. A business transaction
B. A condition arrived at by experience or exercise
C. A series of changes taking place in a defined manner
D. An activity or activities performed to meet defined CMMC objectives
Answer: D (メーッセージを残す)
Understanding the Definition of a "Practice" in CMMC 2.0In CMMC 2.0, the term"practice"refers to specific cybersecurity activities that organizations must implement to achieve compliance with defined security objectives.
* Definition from CMMC Documentation:
* According to theCMMC Model Overview, apracticeis defined as:
Step-by-Step Breakdown:"An activity or activities performed to meet defined CMMC objectives."
* This means that practices are theactions and implementations required to protect Controlled Unclassified Information (CUI) and Federal Contract Information (FCI).
* How Practices Fit into CMMC 2.0:
* CMMC 2.0 Level 1 consists of17 practices, which align withFAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems).
* CMMC 2.0 Level 2 consists of110 practices, aligned directly withNIST SP 800-171 Rev. 2.
* Each practice has anobjectivethat must be met to demonstrate compliance.
* Official CMMC 2.0 References:
* TheCMMC 2.0 Model Documentationdefines practices as "the fundamental cybersecurity activities necessary to achieve security objectives."
* TheCMMC Assessment Process (CAP) Guideoutlines how assessors verify the implementation of these practices during an assessment.
* TheNIST SP 800-171A Guideprovidesassessment objectivesfor each practice to ensure they are implemented effectively.
* Comparison with Other Answer Choices:
* A. A business transaction# Incorrect. CMMC practices focus on cybersecurity activities, not financial or operational transactions.
* B. A condition arrived at by experience or exercise# Incorrect. While practices evolve over time, they are defined activities, not just experience-based conditions.

* C. A series of changes taking place in a defined manner# Incorrect. A practice is a set of security actions, not just a process of change.
結論 :ACMMCの実践とは、定義されたCMMCの目的を達成するために実施される特定のサイバーセキュリティ活動を指します。したがって、選択肢Dが正解です。

最新問題: **31**
LTPを最もよく表しているのは次のうちどれですか？
A. CMMC-AB認定試験プロバイダーとして自社を宣伝する可能性がある
B. 国防総省認可の訓練プログラムを作成する
C. CMMCの知識体系の目標の一部を用いてトレーニングを実施する。
D. CMMC-ABが承認したカリキュラムを指導する
Answer: (解答を表示する)

有効な **CMMC-CCP** 問題集は GoShiken.com が提供された合格しやすい CMMC-CCP 試験問題集！ GoShiken.com が最新の **CMMC-CCP** 試験問題集を提供しています。GoShiken.com CMMC-CCP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CMMC-CCP 問題集をゲットする人はこちら: https://www.goshiken.com/Cyber-AB/CMMC-CCP-mondaishu.html (**23030%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **32**
9月下旬。CA.L2-3.12.1: 組織システムのセキュリティ管理策を定期的に評価し、管理策が適用において効果的であるかどうかを判断します。手順では、セキュリティ管理策の評価を四半期ごとに実施することが規定されています。第2四半期の評価を実施する担当者が現在オフィスを離れており、2時間後にオフィスに戻るため、主任評価担当者には第1四半期の評価レポートのみが提供されます。この情報に基づいて、主任評価担当者は証拠が次のとおりであると判断する必要があります。
A. 十分であり、監査結果をMETと評価する
B. 不十分であり、監査結果を 朱達成」と評価する。
C. 十分であり、第2四半期の評価報告書を検討した後に監査結果を再評価する。
D. 不十分であり、第2四半期の評価報告書を検討した後に監査結果を再評価する。
Answer: (解答を表示する)
管理基準 :CA.L2-3.12.1
CA.L2-3.12.1：組織システムのセキュリティ制御を定期的に評価し、制御が効果的に適用されているかどうかを判断する。」この制御は、NIST SP 800-171の要件3.12.1に基づいています。この要件では、組織がコンプライアンスと有効性を確保するために、定期的なセキュリティ制御評価を実施することを義務付けています。
評価基準と正解の根拠：

証拠レビューおよび評価のタイムライン：
組織の手順書には、セキュリティ管理評価は四半期ごと（3ヶ月ごと）に実施しなければならないと明記されている。
主任評価者は第1四半期の報告書しか入手できないため、評価時点では第2四半期の報告書が欠落している。
CMMC監査要件：
評価者が対照群をMETと評価するためには、評価時に十分な証拠がすぐに利用できる状態である必要がある。
評価時点で第2四半期の報告書が不足しているため、主任評価者は組織が定めた評価頻度への準拠を確認できません。
答えがA、C、Dではない理由：
A（十分、MET）#不正解：管理評価の頻度は四半期ごとですが、第2四半期の証拠が入手できません。遵守状況を確認できません。
C（十分であり、後で再評価する）#誤り：監査中に証拠が入手できない場合、コントロールを最初にMETと評価することはできません。CMMC 2.0には、将来の証拠を待ってコントロールを「条件付き」で合格させる規定はありません。
D（不十分だが、後で再評価する）#誤り：一度コントロールが「NOT MET」と評価されると、新しい監査サイクルで再評価が実施されるまで「NOT MET」のままになります。評価者は、将来の証拠に基づいて評価を遡及的に調整しません。
回答を裏付ける公式CMMC 2.0参照資料：
CMMC評価プロセス（CAP）ガイド（2023年版）：
「管理策がMET（医療環境モニタリング）として評価されるためには、評価対象組織は評価時に十分な証拠を提出しなければならない。」
「証拠が欠落しているか不完全な場合、その評価は「要件を満たしていない」と判断される。」NIST SP 800-171A（セキュリティ要件評価ガイド）
「証拠は、最新のものであり、関連性があり、規定された実施頻度要件への準拠を証明するのに十分でなければならない。」この手続きでは四半期ごとの評価が義務付けられているため、証拠が不足している場合は、準拠を検証することができない。
国防総省CMMCスコープ設定ガイドライン：
「評価者は、評価時に提供された証拠に基づいて判断を下すものとする。必要な証拠が入手できない場合は、管理策は「不適合」と評価されるものとする。」最終結論：
正解はBです。評価時点で必要な証拠（第2四半期報告書）が入手できないため、コンプライアンスを検証するには不十分です。主任評価者は、CMMC 2.0の評価規則に従って、管理策を「未達成」と評価する必要があります。

最新問題: **33**
ある企業が、契約しているCMMCコンサルティング会社のCCP（認定認定専門家）と協力しています。CCPは、ホストユニットがCMMC評価のためにFCI（施設管理情報）とCUI（機密

情報）を文書化する必要がある場所について質問されました。CCPはどのように回答すべきでしょうか？

A. 「SSPでは、資産インベントリ内、およびネットワーク図Yで」

B. 「ネットワーク図、SSP、基本インベントリ内、および提案回答において」

C. 「資産目録、提案書、ネットワーク図」

D. 「ハードウェアインベントリ、データ（下図 ネットワーク図）内」

Answer: A (メーッセージを残す**)**

最新問題**: 34**

CMMCモデル2.0は、どのような規格および規制要件に基づいていますか？

A. NIST SP 800-171およびNIST SP 800-172

B. DFARS、FIPS 100、およびNIST SP 800-171

C. DFARS、NIST、カーネギーメロン大学

D. DFARS、FIPS 100、NIST SP 800-171、およびカーネギーメロン大学

Answer: (解答を表示する**)**

サイバーセキュリティ成熟度モデル認証（CMMC）2.0は、主に米国国立標準技術研究所（NIST）の2つの主要な特別刊行物に基づいています。

NIST SP 800-171 - 「非連邦システムおよび組織における管理対象非機密情報 (CUI) の保護」NIST SP 800-172 - 「管理対象非機密情報を保護するための強化されたセキュリティ要件: NIST 特別刊行物 800-171 の補足」NIST SP 800-171 この文書は CMMC 2.0 の中核となる基盤であり、非連邦システムにおける管理対象非機密情報 (CUI) を保護するためのセキュリティ要件を確立します。

NIST SP 800-171 Rev. 2の110のセキュリティ管理項目は、CMMCレベル2に直接対応しています。

NIST SP 800-172

この補足資料には、高度な持続的脅威（APT）に直面する高価値のCUI（機密情報を扱う組織向けの強化されたセキュリティ要件が含まれています。

これらの強化された要件は、CMMC 2.0モデルにおけるレベル3に適用されます。

B). DFARS、FIPS 100、およびNIST SP 800-171#不正解

DFARS 252.204-7012ではNIST SP 800-171への準拠が義務付けられているが、FIPS 100は関連するサイバーセキュリティ標準としては存在しない。

C). DFARS、NIST、カーネギーメロン大学#不正解

CMMCはDFARSおよびNISTに準拠していますが、カーネギーメロン大学によって開発されたものではなく、また同大学が直接影響を与えたものでもありません。

D). DFARS、FIPS 100、NIST SP 800-171、およびカーネギーメロン大学#誤り。FIPS 100は関係ありませんし、カーネギーメロン大学はCMMCフレームワークの定義エンティティではありません。

CMMC 2.0 スコープガイド（2023年）は、CMMCレベル2がNIST SP 800-171に完全に基づいていることを確認しています。

CMMC 2.0 レベル 3 ドラフト文書では、強化されたセキュリティ要件に関して、NIST SP 800-172 を明示的に参照しています。
国防総省暫定規則（DFARS 252.204-7021）は、組織がCUI保護に関してNIST SP 800-171を満たすことを義務付けています。
参照と分析：誤った選択肢の排除：回答を裏付ける公式の CMMC 2.0 参照資料 最終的な結論：CMMC 2.0 モデルは、NIST SP 800-171 および NIST SP のみから派生しています 800-172となり、Aが唯一の正解となります。

最新問題: **35**
CMMC評価を実施する前に、請負業者はすべての資産を分類することでCMMC評価の範囲を明確にする必要があります。CMMCの実施基準に照らして常に評価される資産カテゴリは次のうちどれですか？
A. CUI資産および特殊資産
B. セキュリティ保護資産およびCUI資産
C. 特殊資産および請負業者リスク管理資産
D. セキュリティ保護資産および請負業者リスク管理資産
Answer: B (メーッセージを残す**)**
CMMC資産スコープ要件の理解CMMCレベル2評価を実施する前に、認証取得を目指す組織（OSC）は、すべての資産を分類することで評価範囲を定義する必要があります。これにより、関連するシステムのみがCMMCの基準に照らして評価され、不要なコンプライアンス負担が軽減されます。
CMMCレベル2のスコープガイドによると、資産カテゴリは4つあります。
* CUI資産 - 管理対象非機密情報（CUI）を処理、保存、または送信する資産。
* セキュリティ保護資産（SPA）- セキュリティ機能を提供する資産（例ファイアウォール、侵入検知システム、ID管理システム）。
* 請負業者リスク管理資産（CRMA）- CUIを直接保存/処理しないが、CUI環境と相互作用する資産（例BYODデバイス、リモートアクセスに使用されるパーソナルコンピュータ）。
* 特殊資産 - 運用技術 (OT)、IoT、政府支給機器 (GFE) などの特殊なシステムで、限定的なCMMC 評価が必要となる場合があります。
常に評価される資産カテゴリーはどれですか？#1. CUI資産（常に評価されます）
* これらはCUIを扱うため、CMMCレベル2の主な焦点となります。
* これらの資産には、NIST SP 800-171 のすべての管理策が適用されます。
#2. セキュリティ保護資産（SPA）（常に評価）
* CUI資産を保護するセキュリティツールは、常に評価に含まれています。
* 例としては、ファイアウォール、ウイルス対策ソフト、エンドポイント検出・対応（EDR）ツール、ID管理システムなどが挙げられます。
* (A) CUI資産および特殊資産#
* CUI資産は評価されますが、特殊資産はCUIセキュリティにおける役割に応じて限定的な方法でのみ評価されます。

* (C) 特殊資産および請負業者リスク管理資産#
* 特殊資産およびCRMAは、CUIセキュリティに直接影響を与えない限り、通常はCMMCコントロールに対して完全に評価されません。
* (D) セキュリティ保護資産および請負業者リスク管理資産#
* SPAは常に評価されますが、CRMAはCUIに直接影響を与えない限り、必ずしも評価されるわけではありません。
* CMMCスコープガイド（レベル2）では、CUI資産とセキュリティ保護資産は常にCMMCの慣行に照らして評価されることが明確に述べられています。
他の選択肢が間違っている理由：CMMCドキュメントからの最終検証：したがって、正解は次のとおりです。
B：セキュリティ保護資産およびCUI資産。

最新問題: **36**
CMMC評価プロセスのどの段階で、証拠の特定、インベントリの取得、および検証を行う作業が含まれますか？
A. フェーズ1：評価の計画と準備
B. フェーズ2：評価の実施
C. フェーズ3：推奨評価結果の報告
D. フェーズ4：未解決の評価問題の是正
Answer: B (メーッセージを残す**)**
CMMC評価プロセスを理解する
CMMC評価プロセス（CAP）は4つのフェーズで構成され、各フェーズにはそれぞれ特定のタスクと目標があります。
フェーズ1：評価の計画と準備 - 評価の計画、スケジュール設定、および準備。
フェーズ2：評価の実施 - 証拠の収集と検証、インタビューの実施、およびコンプライアンスの評価。
フェーズ3：推奨評価結果の報告 - 調査結果を文書化し、結果を報告する。
フェーズ4：未解決の評価問題の是正 - 組織が欠陥に対処できるようにする。
「フェーズ2：評価の実施」が正しい理由とは？
フェーズ2：評価の実施において、評価チームは以下の主要な活動を実施します。
#コンプライアンス検証に必要な証拠を特定する。
#アーティファクト（セキュリティポリシー、構成、ログなど）の取得とレビュー。
#CMMCの実施要件に対する証拠の十分性を検証する。
#主要担当者へのインタビューとサイバーセキュリティの実装状況の観察。
質問には「証拠を特定し、目録を入手し、検証する」と具体的に記載されているため、このタスクはフェーズ2：評価の実施に直接該当します。
回答選択肢の内訳
オプション
説明

正しい？
A) フェーズ1：評価の計画と準備
#誤り - このフェーズは、証拠収集ではなく、スケジュール、ロジスティクス、計画に焦点を当てています。
B) フェーズ2：評価の実施
#正解 - この段階では、証拠の収集、検証、およびレビューを行います。
C) フェーズ3：推奨評価結果の報告
#誤り - このフェーズでは結果を文書化しますが、証拠は収集しません。
D) フェーズ4：未解決の評価問題の是正
#誤り - このフェーズは、証拠収集ではなく、是正措置に焦点を当てています。
CMMC 2.0ドキュメントからの公式参照
CMMC評価プロセスガイド（CAP）-フェーズ2：評価の実施には、証拠の収集と検証などのタスクが明確に含まれています。
最終検証と結論
正解はBです。フェーズ2：評価の実施。このフェーズには、CMMC準拠を判断するために重要な証拠の特定、入手、検証が含まれます。

最新問題: **37**
C3PAO評価計画書には、インタビュー対象者の名前、利用予定の施設、評価の概算費用とスケジュールが記載されています。これは評価計画書のどの部分に該当しますか？
A. リソースを特定し、スケジュールを立てる。
B. 評価チームのメンバーを選定する。
C. 評価リスクを特定し、管理する。
D. 証拠収集方法を選択し、開発する。
Answer: A (メーッセージを残す**)**
認定第三者評価機関（C3PAO）は、CMMCレベル2評価を実施する責任を負います。評価を開始する前に、C3PAOはいくつかの重要な要素を含む評価計画を作成する必要があります。
計画の中で以下の点を捉えている部分：
#インタビュー対象者の名前
#利用予定の施設
#概算費用
#評価スケジュール
これは計画書の『リソースの特定とスケジュールの策定」のセクションに該当します。
手順ごとの詳細：
#1. リソースとスケジュールを特定する
CMMC評価計画のこのセクションでは、以下の概要を説明します。
関係者（例：面接対象者、評価者）。
評価が実施される場所。
タイムラインとスケジュールの詳細。

評価に関連する概算費用。
これにより、必要なリソースがすべて割り当てられ、評価が計画通りに進むことが保証されます。
#2. 他の選択肢が間違っている理由：
Ⓑ）評価チームメンバーの選定#
このセクションでは、評価を実施する評価者の選定に焦点を当てており、面接対象者や施設の一覧は掲載していません。
Ⓒ）評価リスクの特定と管理#
This part of the plandocuments risks(e.g., scheduling conflicts, data access issues), but it doesnot outline names, facilities, or costs.
(D) Select and Develop the Evidence Collection Approach#
This step defineshowevidence will be gathered (e.g., document reviews, interviews, system testing) but doesnot focus on logistics.
Final Validation from CMMC Documentation:
TheCMMC Assessment Process Guidestates thatresource identification and schedulingare essential for organizing the assessment. Since this sectioncaptures interviewees, facilities, costs, and the schedule, the correct answer is:
#A. Identify resources and schedule.

最新問題: **38**
OSCから収集された証拠がレビューされています。評価と組織の範囲に基づいて、主任評価者は評価チームに、ドメイン、プラクティス、ホストユニットによるカバレッジを確認するよう依頼します。
支援組織／ユニットおよびエンクレーブは、各実践項目に対して評価を行うのに十分な包括性を備えています。評価者はどの基準を参照しているのでしょうか？
A. 能力
B. 適切性
C. 十分性
D. 客観性
Answer: C (メーッセージを残す**)**

最新問題: **39**
CMMCレベル1自己評価の準備として、DIB組織のITマネージャーは、会社のSSPで資産の種類を文書化しています。マネージャーは、特定されたマシンコントローラーと組立機を特殊資産として文書化する必要があると判断しました。マネージャーが特定し文書化した特殊資産の種類はどれですか？
A. 試験装置
B. IoT
C. 制限付きIS
D. 運用技術

Answer: (解答を表示する**)**

最新問題**: 40**
CMMC評価プロセスのどの段階で評価計画の策定が含まれますか？
A. フェーズ1
B. フェーズ4
C. フェーズ3
D. フェーズ2
Answer: (解答を表示する**)**

最新問題**: 41**
CMMCモデルにおいて、レベル1にはいくつのプラクティスが含まれていますか？
A. 15の実践
B. 17の実践
C. 72の実践
D. 110の練習
Answer: (解答を表示する**)**
CMMC（サイバーセキュリティ成熟度モデル認証）2.0レベル1は、連邦契約情報（FCI）を保護するために設計されており、17の基本的サイバーセキュリティ対策で構成されています。これらの対策は、FCIを取り扱う請負業者に対する最低限のセキュリティ要件を規定するFAR 52.204-21（対象請負業者情報システムの基本的保護）から直接導き出されたものです。
CMMCレベル1の実践内容の内訳レベル1の17の実践内容は、基本的なサイバーセキュリティ衛生に焦点を当てており、以下の6つの領域に分類されます。
* アクセス制御（AC）- 4つの実践
* AC.L1-3.1.1: システムへのアクセスを許可されたユーザーのみに制限する
* AC.L1-3.1.2: ユーザーによるアクセスを承認されたトランザクションと機能に制限する
* AC.L1-3.1.20: 外部システムへの接続を検証および制御する
* AC.L1-3.1.22: 公開アクセス可能なシステムに掲載または処理される制御情報
* 識別と認証（IA）- 2つの実践
* IA.L1-3.5.1: システムユーザーの識別と認証
* IA.L1-3.5.2: ローカルアクセスおよびネットワークアクセスに多要素認証を使用する
* メディア保護（MP）- 1つの実践例
* MP.L1-3.8.3: 廃棄または再利用する前にメディアを消毒する
* 物理的保護（PE）- 4つの実践
* PE.L1-3.10.1: FCIを含むシステムへの物理的なアクセスを制限する
* PE.L1-3.10.3: 訪問者を案内し、訪問者の行動を監視する
* PE.L1-3.10.4: 物理アクセスの監査ログを維持する
* PE.L1-3.10.5: 物理アクセス機器の制御と管理
* システムおよび通信保護（SC）- 2つの実践

* SC.L1-3.13.1: システム境界における通信の監視と制御
* SC.L1-3.13.5: 公開アクセス可能なシステムコンポーネント用のサブネットワークを実装する
* システムおよび情報インテグリティ（SI）- 4つの実践
* SI.L1-3.14.1: システムの欠陥をタイムリーに特定、報告、修正する
* SI.L1-3.14.2: 指定された場所で悪意のあるコードから保護を提供する
* SI.L1-3.14.4: 悪意のあるコードに対する保護メカニズムを定期的に更新する
* SI.L1-3.14.5: システム コンポーネントのスキャンとリアルタイム ファイル スキャンを実行します。CMMC 2.0 ドキュメントからの公式参照CMMC レベル 1 の 17 のプラクティスは、CMMC 2.0 付録およびレベル 1 の評価ガイド、ならびに FAR 52.204-21 の要件に明示的に記載されています。
これらの対策は、FCI（外国の機密情報）を取り扱うすべての国防総省請負業者が実施しなければならない基本的な安全対策を表しています。
#CMMC 2.0 レベル1の概要:
* 焦点：FCIの基本的な保護
* 練習総数:17
* 出典: FAR 52.204-21
* 評価の種類：自己評価（年次）
最終検証と結論正解はBです。CMMC 2.0の公式文書とFAR 52.204-21の要件から確認された17の実践事項です。

最新問題**: 42**
CMMC評価プロセスのどの段階で評価計画の策定が含まれますか？
A. フェーズ1
B. フェーズ2
C. フェーズ3
D. フェーズ4
Answer: A (メーッセージを残す**)**
CMMC評価プロセスのフェーズを理解するCMMC評価プロセス（CAP）は複数のフェーズで構成されており、各フェーズは評価の異なる側面に焦点を当てています。評価計画の策定は、事前評価フェーズであるフェーズ1で行われます。
* 契約書：OSC（認証を求める組織）と認定第三者評価機関（C3PAO）が評価契約を正式に締結します。
* 評価計画の策定：主任評価者と評価チームは、以下の内容を概説する評価計画を作成します。
* 評価の範囲
* CMMCレベル要件
* 評価方法
* スケジュールとロジスティクス

* 初期データ収集 :システムドキュメント、ポリシー、および関連するセキュリティ制御のレビュー。
第1段階（事前評価段階）における主な活動
* A. フェーズ1 # 正解
* フェーズ1では、評価計画が策定されます。
* 評価開始前に、範囲、方法論、およびロジスティクスについて明確化することを保証します。
* B. フェーズ2 # 不正解
* フェーズ2は評価実施フェーズであり、評価者は証拠を検証し、関係者にインタビューすることで計画を実行します。
* C. フェーズ3 # 不正解
* フェーズ3は事後評価フェーズであり、調査結果を確定し報告書を提出する段階であり、計画を策定する段階ではありません。
* D. フェーズ（不完全な回答）# 不正解
* この質問では特定のフェーズが求められており、正解はフェーズ 1 です。
正解が「フェーズ1」（A）である理由は？
* CMMC評価プロセス（CAP）文書
* フェーズ1は、評価計画が策定される段階と定義します。
* CMMC認定機関（CMMC-AB）ガイドライン
* 計画策定および事前評価活動はフェーズ1で行われることを指定する。
* CMMC 2.0認証ワークフロー
* C3PAOとOSC間の初期協議の一環として、評価計画プロセスを概説する。
この回答を裏付けるCMMC 2.0の参考文献：

最新問題: **43**
CMMCは「実践」をどのように定義していますか？
A. ビジネス取引
B. 経験や訓練によって到達した状態
C. 定められた方法で起こる一連の変化
D. 定義されたCMMCの目標を達成するために実施される活動または複数の活動
Answer: D (メーッセージを残す**)**
CMMC 2.0における「プラクティス」の定義を理解する
CMMC 2.0において、「プラクティス」という用語は、組織が定義されたセキュリティ目標への準拠を達成するために実施しなければならない具体的なサイバーセキュリティ活動を指します。
手順ごとの詳細：
CMMCドキュメントからの定義：
CMMCモデル概要によると、プラクティスは次のように定義されています。
「CMMCの定める目標を達成するために実施される活動、または複数の活動。」

これは、管理対象非機密情報（CUI）および連邦契約情報（FCI）を保護するために必要な行動と実施方法を実践することを意味します。
CMMC 2.0への各プラクティスの適合性：
CMMC 2.0 レベル 1 は 17 の実践項目で構成されており、FAR 52.204-21 (対象となる請負業者の情報システムの基本的な保護) に準拠しています。
CMMC 2.0 Level 2 consists of110 practices, aligned directly withNIST SP 800-171 Rev. 2. Each practice has anobjectivethat must be met to demonstrate compliance.
Official CMMC 2.0 References:
TheCMMC 2.0 Model Documentationdefines practices as "the fundamental cybersecurity activities necessary to achieve security objectives." TheCMMC Assessment Process (CAP) Guideoutlines how assessors verify the implementation of these practices during an assessment.
TheNIST SP 800-171A Guideprovidesassessment objectivesfor each practice to ensure they are implemented effectively.
Comparison with Other Answer Choices:
A). A business transaction# Incorrect. CMMC practices focus on cybersecurity activities, not financial or operational transactions.
B). A condition arrived at by experience or exercise# Incorrect. While practices evolve over time, they are defined activities, not just experience-based conditions.
C). A series of changes taking place in a defined manner# Incorrect. A practice is a set of security actions, not just a process of change.
Conclusion:
ACMMC practicerefers to specificcybersecurity activities performed to meet defined CMMC objectives. This makesOption Dthe correct answer.

最新問題**: 44**
RPOが提供するサービスの中で、最も包括的なサービスは何ですか？
A. アセスメントサービス
B. 研修サービス
C. コンサルティングサービス
D. 教育サービス
Answer: A (メーッセージを残す**)**

最新問題**: 45**
SI.L1-3.14.2 組織の情報システム内の適切な場所で悪意のあるコードからの保護を提供する」を評価する際、OSCのすべてのワークステーションとサーバーに悪意のあるコードからの保護のためのウイルス対策ソフトウェアがインストールされていることが確認されました。ウイルス対策ソフトウェア管理のための集中管理コンソールが設置されており、すべてのデバイスに最新のウイルス対策パターンが適用されていることが記録から示されています。

主任評価者が証拠に関して下すべき最善の判断とは何でしょうか？
A. 十分であり、監査結果はMETと評価できます。
B. 不十分であり、監査結果は「未達成」と評価される。
C. 十分であり、主任評価者はさらなる証拠を求めるべきである。
D. 不十分であり、主任評価者はさらなる証拠を求めるべきである。
Answer: A (メーッセージを残す**)**
SI.L1-3.14.2 の理解: 悪意のあるコードからの保護の提供CMMC レベル 1 プラクティス SI.L1-
3.14.2は、NIST SP 800-171の要件3.14.2に基づいており、組織には以下のことが求められます。
悪意のあるコードに対する対策（例ウイルス対策ソフト、エンドポイントセキュリティソフトウェア）を実施する。
適切な場所（ワークステーション、サーバー、ネットワーク入口など）すべてにおいて、確実にカバー範囲を確保してください。
保護メカニズムを常に最新の状態に保つ（例：定期的な署名更新、ポリシーの適用）。
「MET」評価の評価基準：診療所がMETであるかどうかを判断するために、主任評価者は以下の点を確認する必要があります。
#すべてのワークステーションとサーバーにウイルス対策ソフトウェアまたはエンドポイント保護ソフトウェアがインストールされています。
#このソリューションは一元管理されており、一貫したポリシー適用を保証します。
#署名の更新は最新の状態であり、システムは新たな脅威から保護されています。
#ログまたはレポートは、アクティブな監視と更新を示しています。
正解が「A. 十分であり、監査結果はMETと評価できる」である理由は？提供された証拠は、SI.L1-3.14.2に必要なすべての要件を満たしていることを確認しています。
#すべてのワークステーションとサーバーにウイルス対策ソフトがインストールされています#インストール要件を満たしています。
#集中管理コンソールが導入されています#一貫した執行を保証します。
#記録によると、ウイルス対策シグネチャは最新です#システム保護が最新であることを確認します。
証拠が要件を満たしているため、この慣行はMET（要件を満たしている）と評価されるべきである。
B) 不十分であり、監査結果は「不合格」と評価される可能性があります。# 誤り 提供された証拠は必要な要件をすべて満たしているため、この慣行は「不合格」と評価されるべきではありません。
C) 十分な証拠があり、主任評価者はさらに証拠を求めるべきである # 誤り 十分な証拠が既に存在する場合、追加の証拠は不要です。
D) 不十分であり、主任評価者はさらなる証拠を求めるべきである # 誤り 提供された証拠は管理要件を満たしており、十分である。
他の回答が間違っているのはなぜですか？

CMMC評価プロセス（CAP）文書
十分な証拠が提示された場合、その実践はMETとしてマークできることを規定する。
NIST SP 800-171（要件3.14.2）
アクティブなアップデートを備えたウイルス対策ソフトが満たす、標準的な形式コード保護を定義します。
CMMC 2.0 レベル1（基礎）要件
ウイルス対策ソフトのインストールやアップデートなどの基本的なサイバーセキュリティ対策はSI.L1-のコンプライアンスを満たすことを明確にする。
3.14.2.
この回答を裏付けるCMMC 2.0の参考文献
最終回答：A。十分であり、監査結果はMETと評価できます。

最新問題: **46**
ある企業がプレスリリースを発表しようとしています。AC.L1-3.1.22「公開アクセス可能なシステムに掲載または処理される情報の管理」によると、CMMC要件に対応する際に考慮すべき最も重要な要素は何ですか？
A. 情報が正しい
B. CEOがそのメッセージを承認した
C. 会社はFCIの放出を保護しなければならない
D. FCIの情報のみであれば公開できる
Answer: C (メーッセージを残す**)**
AC.L1-3.1.22には、「公開アクセス可能なシステムに掲載または処理される情報を管理する」と規定されています。この管理策では、組織はFCI（連邦契約情報）が公開されたり、管理されていない方法でアクセス可能になったりしないようにする必要があります。
FCIは、機密情報やCUIでなくても、不正な開示から保護されなければならない。
参照：
NIST SP 800-171、要件3.1.22
CMMCレベル1実践AC.L1-3.1.22
ステップ 2: プレスリリースで FCI を保護することが重要な理由 企業が FCI を含むプレスリリースを発表する場合、その情報が意図せず機密性の高い契約関連データを公開しないようにする必要があります。
FCIには、国防総省が契約に基づいて提供または作成した情報が含まれますが、これらの情報は一般公開を目的としていません。
組織は、意図しない暴露を防ぐための管理策を実施しなければならない。
ステップ3：他の選択肢が間違っている理由A. 情報が正しい（間違い）：
正確性も重要ですが、CMMCの要件は、単に正確性を確保するだけでなく、機密情報を保護することに重点を置いています。
B) CEOがそのメッセージを承認した（誤り）：
CEOの承認は、FCIの保護に対応していないため、CMMC準拠を満たしません。

D) 情報がFCIのみである限り、公開できる（誤り）：
FCIは保護されるべきものであり、国防総省による特別な許可がない限り、公に開示してはならない。
正解の最終確認：会社はFCIを保護し、公式プレスリリースにおいて不正な情報開示が行われないようにしなければならない。
したがって、正解はCです。会社はFCIの放出を保護しなければなりません。

有効な **CMMC-CCP** 問題集は GoShiken.com が提供された合格しやすい CMMC-CCP 試験問題集！ GoShiken.com が最新の **CMMC-CCP** 試験問題集を提供しています。GoShiken.com CMMC-CCP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CMMC-CCP 問題集をゲットする人はこちら: https://www.goshiken.com/Cyber-AB/CMMC-CCP-mondaishu.html (**23030%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **47**
Which phase of the CMMC Assessment Process includes the task to identify, obtain inventory, and verify evidence?
A. Phase 1: Plan and Prepare Assessment
B. Phase 2: Conduct Assessment
C. Phase 3: Report Recommended Assessment Results
D. Phase 4: Remediation of Outstanding Assessment Issues
Answer: A (メーッセージを残す**)**
Understanding the CMMC Assessment ProcessTheCMMC Assessment Process (CAP)consists offour phases, each with specific tasks and objectives.
フェーズ1：評価の計画と準備 - 評価の計画、スケジュール設定、および準備。
フェーズ2：評価の実施 - 証拠の収集と検証、インタビューの実施、およびコンプライアンスの評価。
フェーズ3：推奨評価結果の報告 - 調査結果を文書化し、結果を報告する。
フェーズ4：未解決の評価問題の是正 - 組織が欠陥に対処できるようにする。
「フェーズ2：評価の実施」が正しい理由とは？フェーズ2：評価の実施では、評価チームは以下の主要な活動を実施します。
#コンプライアンス検証に必要な証拠を特定する。
#アーティファクト（セキュリティポリシー、構成、ログなど）の取得とレビュー。
#CMMCの実施要件に対する証拠の十分性を検証する。
#主要担当者へのインタビューとサイバーセキュリティの実装状況の観察。
質問には「証拠を特定し、目録を入手し、検証する」と具体的に記載されているため、このタスクはフェーズ2：評価の実施に直接該当します。
回答選択肢の内訳

説明
正しい？
A) フェーズ1：評価の計画と準備
#誤り - このフェーズは、証拠収集ではなく、スケジュール、ロジスティクス、計画に焦点を当てています。
B) フェーズ2：評価の実施
#正解 - この段階では、証拠の収集、検証、およびレビューを行います。
C) フェーズ3：推奨評価結果の報告
#誤り - このフェーズでは結果を文書化しますが、証拠は収集しません。
D) フェーズ4：未解決の評価問題の是正
#誤り - このフェーズは、証拠収集ではなく、是正措置に焦点を当てています。
CMMC評価プロセスガイド（CAP）-フェーズ2：評価の実施には、証拠の収集と検証などのタスクが明確に含まれています。
CMMC 2.0 ドキュメントからの公式参照最終検証と結論正解は B. フェーズ 2: 評価の実施です。このフェーズには、CMMC 準拠を判断するために重要な証拠の特定、取得、検証が含まれます。

最新問題: **48**
評価プロセスの計画段階で、C3PAOのスタッフは、CMMCレベル2評価を要求したOSCに関連するさまざまな組織をレビューしています。評価に参加するものの、エンタープライズ評価が実施されない限りCMMCレベルを取得できない、本部組織の外部の人、プロセス、およびテクノロジーを表す用語はどれですか？
A. ホストユニット
B. 組織
C. 調整ユニット
D. 支援組織／部署
Answer: D (メーッセージを残す**)**
サイバーセキュリティ成熟度モデル認証（CMMC）評価プロセスにおいては、認証取得を目指す組織（OSC）に関連する様々な主体の役割を、計画段階で理解することが極めて重要です。認定第三者評価機関（C3PAO）のスタッフがCMMCレベル2評価のためにこれらの主体を審査する際には、内部構成要素と外部参加者を明確に区別することが不可欠です。
段階的な説明：
* 本部組織の定義：
* 本部組織とは、国防総省（DoD）との契約に基づきサービスを提供する法人全体を指します。この組織は、CMMC要件への準拠を確保する責任を負います。
* 外部エンティティの識別:
外部組織とは、本部組織の一部ではないものの、本部組織の業務を支援する人、プロセス、および技術を指します。これらの組織は、国防総省契約に関連する機密指定されていない管理情報（CUI）または連邦契約情報（FCI）の取り扱いに関与しているため、評価プロセスに参加します。

* 支援組織／部署の役割：
CMMC評価プロセスの文書によると、支援組織は「本部組織の外部にあり、ホストユニットを支援する人員、手順、および技術」と定義されています。これらの外部組織はホストユニットの運用に不可欠ですが、本部組織の直接的な組織構造には含まれません。
* 評価への影響：
* サポート組織／ユニットはホストユニットのサポートにおいて重要な役割を果たしますが、エンタープライズ評価が実施されない限り、個別のCMMCレベル認証は取得できません。このような場合、評価は本部組織とそのサポート組織の両方を対象とし、関連するすべての組織における包括的なコンプライアンスを確保します。
参考文献：
CMMC評価プロセスの文書では、支援組織とは、ホストユニットを支援する外部組織と定義されています。
サイバーラブ
C3PAOは、支援組織／ユニットの役割を正確に特定し理解することで、評価計画段階で関連するすべての組織が考慮されることを保証し、CMMCレベル2評価の完全性と包括性を維持します。

最新問題: **49**
構成管理（CM）の領域において、必須システム機能を定義する際の基礎となる原則はどれですか？
A. 最も恵まれない人々
B. 重要な懸念事項
C. 最低限の機能
D. 職務分担
Answer: C (メーッセージを残す**)**
CM ドメインにおける最小機能の原則の理解CMMC 2.0 の構成管理 (CM) ドメインは、制御された構成とシステム機能の制限を通じて、組織のシステムのセキュリティと整合性を維持することに重点を置いています。
最小機能の原則とは、システムの機能、サービス、アプリケーションを、本来の目的に必要なものだけに限定することを指します。この原則は、攻撃者に悪用される可能性のある不要なコンポーネントを最小限に抑えることで、攻撃対象領域を縮小します。
CMMCプラクティスCM.L2-3.4.6（最小限の機能の使用）では、「組織のシステムを構成して必要最低限の機能のみを提供するようにすることで、最小限の機能の原則を採用する」と明記されています。その目的は、システム上で不正または不要なアプリケーション、サービス、ポートが実行されないようにすることです。
実装例：
必要のないサービス（リモートデスクトップアクセスなど）は無効にする。
ソフトウェアのインストールを承認済みのアプリケーションに限定する。
未使用のネットワークポートとプロトコルをブロックする。

A) 最も特権の少ない人々
この原則（アクセス制御に関連するもの）は、ユーザーとプロセスが業務を遂行するために必要な最小限のアクセス権限のみを持つことを保証するものです。
これは CMMC プラクティス AC.L2-3.1.5 (最小権限) に関連していますが、システム機能を定義するものではありません。
B) 重要な懸念事項
CMMC、NIST、または関連するフレームワークには、「重要な懸念事項」と呼ばれる公式に認められたサイバーセキュリティ原則は存在しない。
D) 職務の分離
この原則（CMMCAC.L2-3.1.4で規定）は、いかなる個人も重要な機能を無制限に管理できないようにすることで、不正行為や濫用のリスクを低減します。
セキュリティ上は重要だが、システムの必須機能を定義するものではない。
CMMC 2.0 レベル 2 評価ガイド - 構成管理 (CM) ドメイン CM.L2-3.4.6 は、不要な機能を削除してセキュリティを強化するために最小限の機能を義務付けています。
NIST SP 800-171（CMMCの基となる規格） - 要件3.4.6
「システムの機能は、組織の使命または業務機能に必要な基本的な機能のみに制限する」と規定されています。NIST SP 800-53 - コントロール CM-7 (最小機能) では、必要な機能のみで動作するようにシステムを構成するための詳細な推奨事項が提供されています。
正解である最小機能の原則（C）の根拠他の選択肢が不正解である理由公式のCMMCおよびNISTの参照結論最小機能の原則（C）は、CMMC 2.0の構成管理（CM）ドメインにおける必須システム機能を定義するための基礎となります。この原則を適用することで、組織は必要な機能、サービス、およびアプリケーションのみが有効になるようにし、セキュリティリスクを軽減します。

最新問題: **50**
What is a conflict of interest?
A. 透明性の欠如。
B. 法律違反。
C. 認識されている、または実際に起こっている対立。
D. 意図しない情報漏洩。
Answer: C (メーッセージを残す**)**
正解はCです。CMMCエコシステムでは、利益相反を実際の利益相反と認識上の利益相反の両方として扱っているからです。CMMC専門職倫理規定では、CMMCエコシステムのメンバーに対し、実際の利益相反または認識上の利益相反につながる可能性のある活動、慣行、取引への参加を避けるよう求めています。また、利益相反の禁止事項を遵守し、過去の役職や関係が客観性を損なう可能性があるレベル2認証プロセスへの参加をCMMCエコシステムのメンバーに制限しています。
利益相反とは、専門家の判断、独立性、または公平性が、他の利害関係、関係、義務、または過去の活動によって影響を受ける可能性がある、または合理的に見て影響を受ける可能性

がある場合に存在します。CMMCでは、評価の信頼性がコンサルティング機能と認証評価機能の独立性に依存するため、これは特に重要です。たとえば、以前にOSCのサイバーセキュリティプログラムの設計、実装、または修復を支援した評価者またはC3PAOは、後に同じOSCを評価する際に、実際または認識上の利益相反を抱える可能性があります。オプションAは、透明性の欠如が利益相反問題の一因となる可能性はあるものの、定義ではないため誤りです。オプションBは、すべての法的違反が利益相反となるわけではないため、広範すぎます。オプションDは、利益相反ではなく、開示の問題を説明しています。したがって、最良の答えはC、認識上のまたは実際の利益相反です。

最新問題: **51**
OSC（オープンサービスセンター）に対するレベル2評価が実施され、結果の提出準備が整いました。評価結果をアップロードする前に、C3PAO（認定3PAO）はどのような手順を完了する必要がありますか？
A. 査定提出料をお支払いください。
B. 結果の内部レビューを実施する。
C. CMMC-ABに提出予定であることを通知する。
D. 主任評価官とOSCの間で最終ブリーフィングを調整する。
Answer: B (メッセージを残す**)**
ACMMCレベル2評価は、C3PAO（認定第三者評価機関）によって実施され、認証を求める組織（OSC）がNIST SP 800-171で要求されるすべての管理策を満たしているかどうかを判断します。
結果を提出する前に、C3PAOは主任評価者とOSCとの間で最終ブリーフィングを実施し、調査結果を確認し、懸念事項を明確にする必要があります。
A) 評価提出料を支払う#不正解
評価結果の提出には、必須の手数料はかかりません。手数料は評価プロセスにかかるものであり、提出にはかかりません。
B) 結果の内部レビューを完了する#不正解
内部レビューは推奨されるものの、CMMC評価手続きにおいて提出前に必須の手順ではない。
C) CMMC-ABに提出予定であることを通知する.偽
C3PAOはCMMC eMASSシステムを通じてCMMC-ABに結果を提出しますが、事前の通知は必須の手続きではありません。
D) 主任評価者と OSC の間で最終ブリーフィングを調整する#正解 CMMC 評価プロセス (CAP) ガイドラインによると、主任評価者は結果を提出する前に OSC と最終ブリーフィングを実施する必要があります。
このブリーフィングは透明性を確保し、OSCに調査結果に関する洞察を与え、最終的な明確化を可能にする。
CMMC評価プロセス（CAP）v1.0

評価結果を提出する前に、主任評価者とOSC（オンタリオ州セキュリティセンター）の間で最終説明会を実施する必要があります。
CMMC-ABおよびC3PAOのプロセス要件
主任評価者は、CMMC-ABに提出する前に、最終的な調査結果をOSCに伝達しなければならない。
提示された選択肢の分析：正解を裏付ける公式資料　結論：正解は：
#D. 主任評価官とOSCの間で最終ブリーフィングを調整する。

最新問題: **52**
CMMCレベル1の自己評価で、OSCの施設内にFCIを処理、保管、送信しない資産が特定されました。これはどのタイプの資産とみなされますか？
A. FCIアセット
B. 特殊資産
C. 対象外資産
D. 政府発行資産
Answer: C (メーッセージを残す**)**
サイバーセキュリティ成熟度モデル認証（CMMC）2.0フレームワークは、連邦契約情報（FCI）および管理対象非機密情報（CUI）との相互作用に基づいて資産を分類します。CMMCレベル1の自己評価では、資産はFCIを処理、保存、または送信するかどうかに基づいて分類されます。
* FCI資産 - これらの資産はFCIを処理、保存、または送信し、CMMCレベル1のセキュリティ要件（FAR 52.204-21の17のプラクティス）を満たす必要があります。
* CUI資産 - これらの資産は管理された非機密情報（CUI）を取り扱い、NIST SP 800-171に準拠したCMMCレベル2の要件の対象となります。
* 特殊資産 - IoTデバイス、運用技術（OT）、政府支給機器（GFE）、および試験装置が含まれます。これらは、それぞれ固有のサイバーセキュリティ要件があるため、多くの場合、個別に分類されます。
* 対象外資産 - FCIまたはCUIを処理、保存、または送信しない資産。これらはCMMCの慣行に準拠する必要はありません。
* 政府発行資産 - これらは、契約固有の目的のために政府から提供される資産であり、多くの場合、政府の方針に基づく遵守が求められます。
* この質問では、特定された資産がFCIを処理、保存、または送信しないことが明記されています。
* CMMC 2.0のガイドラインによると、FCIまたはCUIを扱う資産のみがセキュリティ管理の対象となります。
* OSCの施設内に物理的に存在するが、FCIまたはCUIと相互作用しない資産は、「対象外資産」のカテゴリに分類されます。
* これらの資産は、FCIまたはCUIのセキュリティに影響を与えないため、CMMC固有のサイバーセキュリティ制御を必要としません。

* CMMC スコープガイド (2021 年 11 月) - スコープ外の資産とは、OSC の環境内にあるが、FCI または CUI と相互作用しない資産と定義されています。
* CMMC 2.0 レベル 1 ガイド - FCI 資産に対するセキュリティ コントロールのみを要求しており、FCI を処理、保存、または送信しない資産は対象外です。
* CMMC評価プロセス（CAP）ガイド - OSC環境における資産の分類を特定し、コンプライアンス要件を決定します。
CMMC 2.0 に基づく資産カテゴリ: 正解が C. 範囲外資産である理由: 関連する CMMC 2.0 の参照: 最終的な正当化: 資産は FCI を処理、保存、または送信しないため、範囲外資産には該当しません。
「FCI資産」または「特殊資産」。政府発行の資産でもありません。したがって、CMMC 2.0 における正しい分類は「対象外資産（C）」です。

最新問題**: 53**
Exercising due care to ensure the information gathered during the assessment is protected even after the engagement has ended meets which code of conduct requirement?
A. Availability
B. Confidentiality
C. Information Integrity
D. Respect for Intellectual Property
Answer: (解答を表示する**)**
The requirement to exercise due care in protecting information gathered during an assessment aligns with the principle ofConfidentialityunder theCMMC Code of Professional Conduct (CoPC). This ensures that sensitive assessment data, findings, and any Controlled Unclassified Information (CUI) remain protected even after the engagement concludes.
Step-by-Step Breakdown:
Definition of Confidentiality in CMMC Context:
Confidentiality refers to protecting sensitive information from unauthorized disclosure.
In the context of a CMMC assessment, it includes safeguarding assessment artifacts, findings, and other sensitive data collected during the evaluation process.
CMMC Code of Professional Conduct (CoPC) References:
TheCMMC Code of Professional Conductstates that assessors and organizations must handle all collected information with discretion andensure its protection post-engagement.
Clause on"Maintaining Confidentiality"specifies that assessors must:
Not disclose sensitive information to unauthorized parties.
Secure data in storage and transmission.
Retain and dispose of data securely in accordance with federal regulations.
Alignment with NIST 800-171 & CMMC Practices:
CMMC Level 2 incorporates NIST SP 800-171 controls, which include:

Requirement 3.1.3:"Control CUI at rest and in transit" to ensure unauthorized individuals do not gain access.
Requirement 3.1.4:"Separate the duties of individuals to reduce risk" ensures that assessment findings are only shared with authorized personnel.
These requirements align with the duty toexercise due carein protecting assessment-related information.
Why the Other Options Are Incorrect:
(A) Availability:This refers to ensuring data is accessible when needed but does not directly relate to protecting gathered information post-assessment.
(C) Information Integrity:This focuses on preventing unauthorized modifications rather than restricting disclosure.
(D) Respect for Intellectual Property:While related to ethical handling of proprietary data, it does not directly cover post-engagement confidentiality requirements.
Final Validation from CMMC Documentation:
TheCMMC Code of Professional ConductandNIST SP 800-171control requirements confirm thatConfidentialityis the correct answer, as it directly pertains to protecting information post-assessment.
Thus, the correct answer isB. Confidentiality.

最新問題**: 54**
OSC（オープンサービスセンター）に対するレベル2評価が実施され、結果の提出準備が整いました。評価結果をアップロードする前に、C3PAO（認定3PAO）はどのような手順を完了する必要がありますか？
A. 結果の内部レビューを実施する。
B. 査定提出料をお支払いください。
C. CMMC-ABに提出予定であることを通知する。
D. 主任評価官とOSの間で最終ブリーフィングを調整する
Answer: A (メーッセージを残す**)**

最新問題**: 55**
SC.L2-3 13.14: VoIP技術の使用を制御および監視することは、OSCの評価において「適用外」とされています。これは評価範囲にどのような影響を与えますか？
A. VoIP技術を使用していない場合でも、既存の電話システムはすべて対象となります。
B. 誤りが発生しましたので、主任評価者に連絡して誤りを訂正してください。
C. VoIP技術は対象範囲内であり、FIPS検証済みの暗号化を使用しているため、評価する必要はありません。
D. VoIP技術は対象範囲内で使用されていないため、この実践に対する評価手順は規定されていません。
Answer: D (メーッセージを残す**)**

SC.L2-3.13.14 の理解 - VoIP テクノロジーの使用の制御と監視CMMC 2.0 レベル 2 の要件SC.L2-3.13.14 は、NIST SP 800-171、セキュリティ要件から来ています。
3.13.14では、組織は自社のシステム境界内で使用されるVoIP（Voice over Internet Protocol）技術の使用を管理および監視しなければならないと規定しています。
システムがVoIP技術を使用していない場合、評価すべきものがないため、この制御は適用されません（N/A）。
選択肢Dが正解である理由
要件が「該当なし（N/A）」とマークされている場合、それはOSCが評価範囲内でその管理策の対象となる技術またはプロセスを使用していないことを意味します。
評価対象となるVoIPシステムが存在しないため、評価手順は不要です。
オプション A（既存の電話システムが対象範囲に含まれる）は、従来の（VoIP ではない）電話システムは SC の対象外であるため、誤りです。L2-3.13.14 - VoIP のみが対象範囲に含まれます。
オプションB（エラー、主任評価者に連絡してください）は誤りです。VoIPを使用しない場合、SC.L2-3.13.14をN/Aとマークすることは有効です。これはエラーではありません。
オプションC（VoIPは対象範囲内だが、FIPS認証済みの暗号化を使用しているため、評価する必要はない）は誤りです。VoIPがFIPS認証済みの暗号化を使用している場合でも、監視と使用制御が適切に行われていることを確認するために、制御を評価する必要があります。
CMMC公式ドキュメントの参照
CMMC 2.0 レベル2評価ガイド - SC.L2-3.13.14
NIST SP 800-171、セキュリティ要件3.13.14
CMMCスコープ設定ガイダンス - 適用対象外（N/A）のプラクティスの決定
最終確認
OSCのシステム境界内でVoIPが使用されていない場合、制御の評価は不要となるため、オプションDが正解となります。

最新問題: **56**
CMMCレベル2評価における請負業者のスコープ要件は、資産をインベントリ、SSP、およびネットワーク図に文書化することであり、これは以下に適用されます。
A. 請負業者リスク管理資産および特殊資産。
B. 対象外資産を除くすべての資産カテゴリ。
C. CUIおよびセキュリティ保護資産のカテゴリ。
D. GUIアセット。
Answer: B (メーッセージを残す)

最新問題: **57**
An Assessment Team is conducting interviews with team members about their roles and responsibilities. The team member responsible for maintaining the antivirus program

knows that it was deployed but has very little knowledge on how it works. Is this adequate for the practice?

A. Yes, the antivirus program is available, so it is sufficient.

B. Yes, antivirus programs are automated to run independently.

C. No, the team member must know how the antivirus program is deployed and maintained.

D. No, the team member's interview answers about deployment and maintenance are insufficient.

Answer: C (メーッセージを残す)

For a practice to beadequately implementedin aCMMC Level 2 assessment, theresponsible personnel must demonstrate knowledge of deployment, maintenance, and operationof security tools such asantivirus programs. Simply having the tool in place isnot sufficient-there must be evidence that it isproperly configured, updated, and monitoredto protect against threats.

Step-by-Step Breakdown:#1. Relevant CMMC and NIST SP 800-171 Requirements

* CMMC Level 2 aligns with NIST SP 800-171, which includes:
* Requirement 3.14.5 (System and Information Integrity - SI-3):
* "Employautomatedmechanisms toidentify, report, and correctsystem flaws in a timely manner."
* Requirement 3.14.6 (SI-3(2)):
* "Employautomated toolsto detect and prevent malware execution."
* These requirements imply that theperson responsible for antivirus must understand how it is deployed and maintainedto ensure compliance.

#2. Why the Team Member's Knowledge is Insufficient

* Antivirus tools requireregular updates,configuration adjustments, andmonitoringto function properly.
* The responsible team member must:
* Knowhow the antivirus was deployedacross systems.
* Be able toconfirm updates, logs, and alerts are monitored.
* Understand how torespond to malware detectionsand failures.
* If the team member lacks this knowledge, assessors maydetermine the practice is not fully implemented.

#3. Why the Other Answer Choices Are Incorrect:

* (A) Yes, the antivirus program is available, so it is sufficient.#
* Incorrect:Just having antivirus softwareinstalleddoes not prove compliance. It must bemanaged and maintained.
* (B) Yes, antivirus programs are automated to run independently.#
* Incorrect:While automation helps, security toolsrequire oversight, updates, and configuration.
* (D) No, the team member's interview answers about deployment and maintenance are insufficient.#

* Partially correct but incomplete:Themain issueis that the team membermust have sufficient knowledge, not just that their answers are weak.
Final Validation from CMMC Documentation:TheCMMC Assessment Guide for SI-3 and SI-3(2)states that personnel mustunderstand the function, deployment, and maintenance of security toolsto ensure proper implementation.
Thus, the correct answer is:

最新問題**: 58**
組織システムの範囲を定める際、サイバーセキュリティCUIプラクティスの適用範囲は、以下のコンポーネントに適用されます。
A. CUIを処理、保存、または送信する連邦システム。
B. CUIを処理、保存、または送信する非連邦システム。
C. CUIを処理、保存、または送信する連邦システム、またはシステムコンポーネントを保護するシステム。
D. CUIを処理、保存、または送信する非連邦システム、またはシステムコンポーネントを保護するシステム。
Answer: D (メーッセージを残す**)**
CMMC 2.0におけるスコープ設定の理解
CMMC 2.0フレームワークは、CUIを処理、保存、または送信する非連邦システムに適用されます。
スコープ設定によって、どのシステムコンポーネントがCMMCの基準に準拠する必要があるかが決定されます。
システムがCUI（機密情報を処理、保存、または送信する場合、あるいはこれらのシステムのセキュリティを提供する場合は、評価範囲に含める必要があります。
正解が D. CUIを処理、保存、または送信する、あるいはシステムコンポーネントを保護する非連邦システム」である理由は？
CMMCは請負業者に適用され、連邦政府のシステムには適用されない。
CMMCは、国防総省（DoD）の請負業者向けに設計されており、連邦政府のシステム向けではありません。
連邦政府のシステムは既にNIST SP 800-53およびその他の規制によって管理されている。
対象範囲には、CUIを処理するシステムと、それらを保護するシステムの両方が含まれます。
CUIを処理、保存、または送信するシステムは対象範囲に含まれる。
Systems thatprovide protection for CUI systems(e.g., firewalls, monitoring tools, security appliances) arealso in scope.
Why Not the Other Options?
A). Federal systems that process, store, or transmit CUI.#Incorrect
CMMCdoes not apply to federal systems.
B). Nonfederal systems that process, store, or transmit CUI.#Partially correct but incomplete Itexcludes security systemsthat protect CUI assets, whichare also in scope.

C). Federal systems that process, store, or transmit CUI, or that provide protection for the system components.
#Incorrect
CMMConly applies to nonfederal systems.
Relevant CMMC 2.0 References:
CMMC Scoping Guide (Nov 2021)- Confirms that CMMCapplies to nonfederal systemsprocessingCUI.
NIST SP 800-171 Rev. 2- Specifies security requirements fornonfederal systemshandling CUI.
DFARS 252.204-7012- Requires DoD contractors to implementNIST SP 800-171onnonfederal systemshandling CUI.
Final Justification:
SinceCMMC applies to nonfederal systems that process CUI or protect those systems, the correct answer isD.
Nonfederal systems that process, store, or transmit CUI, or that provide protection for the system components.

最新問題**: 59**
The Assessment Team has completed the assessment and determined the preliminary practice ratings. The preliminary practice ratings must be shared with the OSC prior to being finalized for submission. Based on this information, the assessor should present the preliminary practice ratings:
A. During the final Daily Checkpoint
B. After discussing with the CMMC-AB
C. Via email after the final Daily Checkpoint
D. Over the phone after the final Daily Checkpoint
Answer: (解答を表示する**)**
According to the CMMC Assessment Process (CAP) v2.0, assessors are required to conduct Daily Checkpoint Meetings at the end of each day to summarize progress with the OSC (Organization Seeking Certification).
The final Daily Checkpoint is where preliminary practice ratings are shared, before the quality assurance review and Out-Brief. The Out-Brief is reserved for the presentation of final results. Additionally, Department of Defense regulations (32 CFR 170.17(c)(2)) provide a 10-business-day re-evaluation window for requirements marked NOT MET before the final report is delivered, which necessitates that the OSC see preliminary ratings during the assessment process itself.
Supporting Extracts from Official Content:
CAP v2.0, 2.23: "The assessment team shall host a Daily Checkpoint Meeting with the OSC at the end of each assessment day to summarize progress." CAP v2.0, 3.7: "The C3PAO shall conduct the quality assurance review... prior to the conduct of the Out- Brief

Meeting." CAP v2.0, 3.10: "The purpose of the Out-Brief Meeting is to convey the results of the assessment to the OSC."
32 CFR 170.17(c)(2): "A security requirement assessed as NOT MET may be re-evaluated... for 10 business days... if the CMMC Assessment Findings Report has not been delivered." Why Option A is Correct:
The CAP specifies that Daily Checkpoint Meetings are the formal, structured mechanism for assessors to communicate progress and preliminary findings to the OSC.
The final Daily Checkpoint provides the OSC with visibility into the preliminary practice ratings before they are finalized, ensuring transparency and alignment.
The Out-Brief is explicitly for conveying the final assessment results after the C3PAO has completed QA.
Federal regulation (32 CFR 170.17(c)(2)) requires the OSC to have access to preliminary results so they can provide additional evidence for re-evaluation before the report is locked, further confirming that this exchange must occur at the final Daily Checkpoint.
References (Official CMMC v2.0 Content):
CMMC評価プロセス（CAP）v2.0 :セクション2.23（日々のチェックポイント）、3.7〜3.10（品質保証と最終報告）。
32 CFR 170.17(c)(2): セキュリティ要件の再評価期間。
DoD CMMC評価ガイド - レベル2（v2.13）MET/NOT MET判定および所見に関するガイダンス。

最新問題**: 60**
CCP（認定認定プロバイダー）が、評価チームとともにCMMCレベル2の初回評価を受けており、自身の責任を理解するためにCMMC評価プロセスを見直しています。理解を促進し、明確化を図るために、主題専門家から情報を収集する最適な方法はどれですか？
A. テスト
B. 検査する
C. インタビュー
D. 評価
Answer: C (メーッセージを残す**)**
CMMC評価方法の理解CMMC評価プロセス（CAP）では、サイバーセキュリティ対策への準拠を確認するために使用される3つの主要な評価方法が定義されています。
* 調査 - 文書、ポリシー、構成、ログを確認します。
* インタビュー - プロセスを明確にし、実装を確認するために、主題分野の専門家（SME）と対話する。
* テスト - システム構成やセキュリティ対策などの技術的な実装を観察する。
この質問は、理解を深め、明確化を図るために中小企業から情報を収集する方法を求めているため、正しい方法はインタビューです。
なぜ「インタビュー」が正しいのか？#インタビューは、中小企業から情報を収集し、理解を確認し、セキュリティプロセスを明確にするために特別に設計されています。

#CMMC評価ガイドでは、評価者はサイバーセキュリティ対策を担当する主要な担当者にインタビューを行う必要があります。
#調査（オプションB）とテスト（オプションA）も有効な評価方法ですが、中小企業から直接知見を収集することに重点を置いていません。
回答選択肢の内訳
説明
正しい？
A: テスト
#誤り - この方法は技術的な検証を伴うものであり、専門家の知見を収集するものではありません。
B：検査する
#誤り - この方法は文書レビューに重点を置いており、SME（中小企業）とのやり取りには重点を置いていません。
C :インタビュー
#正解 - 中小企業から情報を収集し、明確化を図るために使用される方法。
D：評価
#誤り - これは一般的な用語であり、特定の評価方法ではありません。
* CMMC評価プロセスガイド（CAP）- インタビューを中小企業から情報を得る方法として定義しています。
CMMC 2.0 ドキュメントからの公式参照最終検証と結論正解は C. インタビューです。この方法は、サイバーセキュリティの実装を検証するために、主題専門家から洞察を収集します。

最新問題: **61**
「評価チームは適切な証拠を持っているか？」という質問に答えるために、どのような基準が使用されますか？
A. 妥当性基準
B. 客観性基準
C. 十分性基準
D. 主観性基準
Answer: (解答を表示する**)**
CMMC 2.0の評価においては、十分性基準は、評価チームが特定の要件への準拠に関する結論を裏付けるのに十分な証拠を収集したかどうかを判断するために使用されます。
十分性基準の定義：
十分性とは、評価中に収集された証拠の量と完全性を指します。
これにより、収集された証拠が、コンプライアンスの客観的かつ妥当な判断を裏付けるのに十分であることが保証されます。
CMMC 2.0において十分性が重要な理由：
評価者は、収集された証拠の量が、疑義や欠落なく調査結果を裏付けるのに十分であることを確認しなければならない。

これにより、組織がコンプライアンスを主張しながらも、それを証明するために必要な文書、技術的証拠、または手続き上の検証が不足している状況を防ぐことができます。
CMMC 2.0の公式参考資料：
CMMC評価プロセス（CAP）ガイドでは、評価結果を検証する上での重要な要素として十分性を定義しています。
CMMC 2.0 レベル2 スコープ設定ガイダンスによると、評価者は成果物、文書、インタビュー、システム構成をレビューする際に、十分性基準を適用しなければならない。
国防総省のCMMC評価ガイド（NIST SP 800-171Aに準拠）は、コンプライアンスに関する決定は、十分な量の検証可能な証拠によって裏付けられなければならないことを強調している。
他の基準との比較：
妥当性基準# 証拠の量ではなく質に焦点を当てます。
客観性基準# 証拠が偏りがなく公平であることを保証するが、必ずしも完全であるとは限らない。
主観性基準# 評価は客観的で事実に基づいた証拠に基づかなければならないため、CMMCには適用されません。
手順ごとの詳細：結論CMMC 2.0 の評価において準拠を確認するには、評価チームは判断を裏付ける十分な証拠が利用可能であることを確認する必要があります。したがって、「十分性基準」（選択肢C）が正解となります。

有効な **CMMC-CCP** 問題集は GoShiken.com が提供された合格しやすい CMMC-CCP 試験問題集！ GoShiken.com が最新の **CMMC-CCP** 試験問題集を提供しています。GoShiken.com CMMC-CCP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CMMC-CCP 問題集をゲットする人はこちら: https://www.goshiken.com/Cyber-AB/CMMC-CCP-mondaishu.html (**23030%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード**: Freepdfdumps**)

最新問題**: 62**
As part of CMMC 2.0, the change to Level 1 Self-Assessments supports "reduced assessment costs" allows all companies at Level 1 (Foundational) to:
A. to conduct self-assessments.
B. opt out of CMMC Assessments.
C. have assessment costs reimbursed by the DoD.
D. pay no more than $500.00 for their annual assessment.
Answer: (解答を表示する**)**
Step 1: Review CMMC 2.0 Reforms (Level 1 - Foundational)As part ofCMMC 2.0, the DoD announced changes toreduce burden and costsfor companies that only handleFederal Contract Information (FCI):

DoD Statement (CMMC 2.0 Overview):
"Level 1 (Foundational) will only require an annual self-assessment, affirming implementation of the 17 FAR
52.204-21 controls."
#Step 2: Intent of "Reduced Assessment Costs"The move to allowself-assessments at Level 1was explicitly designed toeliminate the costof hiring third-party assessors for organizations that only handle FCI.
Level 1 self-assessments are:
Conductedinternally by the OSC,
Affirmed annuallyby a senior company official,
Submitted via SPRS(Supplier Performance Risk System).
B). Opt out of CMMC Assessments# Incorrect. Organizations must still perform aself-assessmentannually - they cannot opt out entirely.
C). Have assessment costs reimbursed by the DoD# No such reimbursement mechanism exists.
D). Pay no more than $500.00...# No such fixed cost is set or guaranteed in CMMC documentation.
#Why the Other Options Are Incorrect
UnderCMMC 2.0, all companies atLevel 1 (Foundational)are permitted toconduct self-assessmentsannually to demonstrate compliance, supporting the DoD's goal ofreducing assessment costsfor low-risk contractors.

最新問題**: 63**
担当者が割り当てられた情報セキュリティ関連の職務と責任を遂行できるよう訓練を受けることを義務付けるという要件は、最初にどこに記載されていますか？
A. レベル1
B. レベル2
C. レベル3
D. 全レベル
Answer: B (メーッセージを残す**)**
CMMCにおけるトレーニング要件の理解担当者が割り当てられた情報セキュリティ関連の職務と責任を遂行するためのトレーニングを受けることを保証するという要件は、CMMCレベル10で初めて登場します。
2NIST SP 800-171 管理 AT.L2-3.2.1 の一部として。
トレーニング要件に関する重要な詳細 #AT.L2-3.2.1：「担当者が割り当てられた情報セキュリティ関連の職務と責任を遂行できるよう、トレーニングを実施すること。」
#この管理策はNIST SP 800-171に基づいており、CMMCレベル2（高度）に適用されます。
#これにより、機密指定されていない管理情報（CUI）を取り扱う従業員が、サイバーセキュリティに関する責任を理解していることが保証されます。
* A. レベル1 # 不正解

* CMMCレベル1には、このトレーニング要件は含まれていません。レベル1は、連邦契約情報（FCI）の基本的な保護に重点を置いていますが、正式なサイバーセキュリティトレーニングは要求していません。
* B. レベル2 # 正解
* トレーニング要件（AT.L2-3.2.1）は、NIST SP 800-171に準拠したCMMCレベル2で初めて登場します。
* C. レベル3 # 不正解
* トレーニング要件は既にレベル2に存在します。レベル3はレベル2をベースに、追加のリスク管理と高度なサイバーセキュリティ対策を導入していますが、トレーニングはレベル2で導入されます。
* D. 全レベル # 不正解
* CMMCレベル1にはこの要件は含まれていません。この要件はレベル2で初めて導入されます。
正解が「B. レベル2」である理由は？
* NIST SP 800-171（要件3.2.1）
* CUIを取り扱う人員に対する必須の研修要件を定義する。
* CMMCレベル2評価ガイド
* AT.L2-3.2.1 をレベル 2 の必須実践項目としてリストしています。
* CMMC 2.0 モデルの概要
* CMMCレベル2がNIST SP 800-171に準拠していることを確認します。NIST SP 800-171には、セキュリティトレーニングの要件が含まれています。
この回答を裏付けるCMMC 2.0の参考文献：

最新問題: **64**
内部告発者が連邦政府を代表して訴訟を起こすことを認めている規制はどれですか？
A. 虚偽請求法
B. NISTSP 800-171
C. 職業倫理規定
D. NISTSP 800-53
Answer: (解答を表示する**)**

最新問題: **65**
OSCを用いた評価の範囲設定において、FCIおよび/またはCUIの存在を最も適切に判断できる文書はどれですか？
A. OSC SSP
B. OSC POA&M
C. OSC証拠
D. OSCと国防総省との契約
Answer: D (メーッセージを残す**)**

DFARS条項252.204-7012の理解国防連邦調達規則補足（DFARS）条項252.204-7012は、機密指定されていない管理情報（CUI）を含むすべての国防総省契約および入札で要求される必須のサイバーセキュリティ条項です。
DFARS 252.204-7012# の主な要件は、CUI を扱う請負業者向けに NIST SP 800-171 セキュリティ管理を実装することです。
#サイバーインシデント発生後72時間以内に国防総省サイバー犯罪センター（DC3）に報告する必要があります。
#国防総省の情報システムを保護するための適切なセキュリティ対策を義務付ける。
#COTS品のみを調達する契約を除く、すべての国防総省契約に適用されます。
オプションA（正解）CUIが関係する場合、DFARS 252.204-7012はすべての国防総省の契約および入札に含めなければなりません。
選択肢B（誤り）FARパート12の手続きは商用物品の調達に適用されますが、DFARS 7012は調達手続きに関係なく適用されます。
選択肢C（誤り）：市販品（COTS）のみを対象とした契約はDFARSの適用対象外です。
7012。
選択肢D（誤り）：改造せずに販売されるCOTS品にはDFARS 7012を含める必要はありません。
DFARS条項252.204-7012（保護対象防衛情報およびサイバーインシデント報告の保護）NIST SP 800-171 - DFARS 7012に基づく請負業者に義務付けられているサイバーセキュリティ基準。
「すべての国防総省の入札および契約」が正しい理由とは？国防総省およびDFARS文書からの公式参照最終検証と結論

最新問題: **66**
IT マネージャーは、会社の CMMC レベル 1 自己評価の範囲を定めています。マネージャーは、FCI を保存、処理、または送信するために使用されているサーバー、ラップトップ、データベース、およびアプリケーションを検討します。IT マネージャーが検討している資産の種類はどれですか?
A. ESP
B. 人々
C. 設備
D. テクノロジー
Answer: D (メーッセージを残す**)**
CMMC 2.0における資産タイプの理解CMMC 2.0では、資産は連邦契約情報（FCI）または管理対象非機密情報（CUI）の取り扱いにおける役割に基づいて分類されます。レベル1およびレベル2のサイバーセキュリティ成熟度モデル認証（CMMC）スコープガイダンスでは、組織が保護が必要な資産を特定するのに役立つ資産定義が提供されています。
CMMCスコープ設定ガイダンスによると、主な資産タイプは5つあります。
* セキュリティ保護資産（ESP - 外部サービスプロバイダーおよびセキュリティシステム）
* 関係者（FCI/CUIと接する職員）

* 施設（FCI/CUI収容施設の所在地）
* テクノロジー（FCI/CUIを保存、処理、または送信するハードウェア、ソフトウェア、およびネットワーク）
* CUI 資産 (レベル 2 の評価では、CUI を特に保存する資産) なぜ「テクノロジー」が正解なのか IT マネージャーは、サーバー、ラップトップ、データベース、アプリケーションを評価しています。これらはすべて、FCI を保存、処理、または送信するために使用されるテクノロジー資産です。
CMMCスコープ設定ガイダンスによると、テクノロジー資産には以下が含まれます。
#エンドポイント（ノートパソコン、ワークステーション、モバイルデバイス）
#サーバー（オンプレミスまたはクラウドベース）
#ネットワーク機器（ルーター、ファイアウォール、スイッチ）
#アプリケーション（ソフトウェア、クラウドベースツール）
#データベース（FCIまたはCUIの保存）
ITマネージャーはこれらのコンポーネントに焦点を当てているため、正しい資産カテゴリはテクノロジー（オプションD）です。
* A. ESP (セキュリティ保護資産)#誤り。ESPとは、FCI/CUIの保護に役立つセキュリティ関連資産（ファイアウォール、監視ツール、マネージドセキュリティサービスなど）を指しますが、FCI/CUIを直接保存、処理、または送信するものではありません。
* B. 人#不正解。従業員はFCIの処理において役割を果たしますが、この質問はハードウェアとソフトウェアに焦点を当てており、これらはテクノロジーの範疇に属し、人の範疇には含まれません。
* C. 施設#不正解。施設とは、FCI/CUIが保管または処理される物理的な建物またはセキュリティで保護された区域を指します。質問では、サーバー、ラップトップ、アプリケーションが明示的に言及されていますが、これらは物理的な施設ではありません。
他の回答が間違っている理由
* CMMCレベル1スコープガイド（CMMC-AB）- テクノロジーを含む資産カテゴリを定義します。
* CMMC 2.0 評価者向けスコープ設定ガイダンス - FCI 資産に関する明確化を提供します。
CMMC公式資料によると、オプションD（テクノロジー）が最も正しい選択肢です。
2.0ガイダンス。

最新問題**: 67**
A CCP is working as an Assessment Team Member on a CMMC Level 2 Assessment. The Lead Assessor has assigned the CCP to assess the OSC's Configuration Management (CM) domain. The CCP's first interview is with a subject-matter expert for user-installed software. With respect to user-installed software, what facet should the CCP's interview focus on?
A. Controlled and monitored
B. Removed from the system
C. Limited to mission-essential use only

D. Scanned for malicious code
Answer: C (メーッセージを残す**)**

最新問題**: 68**
C3PAOは、OSCの評価後、限定的な業務上の不備是正評価を完了しました。主任評価者は、不備をPOA&Mに移行することを推奨しましたが、OSCは暫定認証のままとなります。この措置を開始するために、METと評価される必要のある業務の最小数はいくつですか？
A. 88の実践
B. 80の練習
C. 110の実践例
D. 100の実践
Answer: A (メーッセージを残す**)**

最新問題**: 69**
OSCは、脆弱性スキャンが実施されたことを示す文書を提出しなければならない。
A. OSCが定める頻度で、新たな脆弱性が発見された場合。
B. 認定RPOによって定義される。
C. 侵入テストが実行されるたびに。
D. 必要に応じて、またはセキュリティマネージャーの指示に従って実施します。
Answer: (解答を表示する**)**
正解はAです。CMMC 2.0レベル2の要件RA.L2-3.11.2 脆弱性スキャン」では、組織は 組織のシステムとアプリケーションの脆弱性を定期的に、また、それらのシステムとアプリケーションに影響を与える新たな脆弱性が特定されたときにスキャンする」ことが求められています。公式のCMMCモデル概要では、この要件がNIST SP 800-171 Rev. 2、3.11.2に直接対応付けられています。公式のCMMCレベル2評価ガイドでは、これをさらに評価目標に細分化しています。組織は脆弱性スキャンの頻度を定義し、定義された頻度で組織のシステムとアプリケーションのスキャンを実行し、新たな脆弱性が特定されたときにスキャンを実行する必要があります。
したがって、OSC は、脆弱性スキャン スケジュール、スキャン レポート、ツール出力、手順、ポリシー、チケットなどの証拠を保持し、スキャンが組織で定義された頻度で実行され、新しい脆弱性が特定されたことを示す必要があります。オプション B は、RPO が助言または支援を行うことはできますが、CMMC 要件ではスキャン頻度が 認定された RPO によって定義される」とは規定されていないため、誤りです。オプション C は、脆弱性スキャンが侵入テスト イベントに限定されないため、誤りです。オプション D は、純粋にアドホック スキャンまたはセキュリティ マネージャーの指示があった場合にのみスキャンを行うだけでは、頻度を定義して従うという要件を満たさないため、誤りです。

最新問題**: 70**

OSCが今後の評価のために証拠を提出しました。評価者はその証拠を審査し、CMMCの基準を満たすには不十分であると判断しました。評価者はどのような対応を取ることができますか？
A. CMMC-ABに通知する。
B. 評価をキャンセルする。
C. 評価を延期する。
D. C3PAOに連絡して指導を受けてください。
Answer: C (メーッセージを残す)
CAP v2.0では、「評価準備状況」がフェーズ1（事前評価の実施）の正式なゲートとなっています。フェーズ1の目的は、C3PAOがOSCがレベル2セキュリティ要件の評価に向けて十分な準備をしているかどうかを評価することです。評価前に提出された証拠が不十分で、OSCが評価を進める準備ができていないと判断された場合、CAPでは評価準備状況の不利な決定について規定しています。主任CCAは承認担当官に通知し、是正措置に関する助言を与えることなく、評価の中止を勧告する理由を文書で説明する必要があります。CAPは次に、OSCが評価を中止または延期することを決定した場合、両当事者は合意に従って（機密情報の返還を含め）問題を解決し、OSCの準備が整った時点で評価の見直しについて話し合うべきであると述べています。これは、最適な回答である「評価を延期する」に直接対応します。
他の選択肢はCAPの規定された処理方法と一致しません。CAPは、通常の証拠不十分（A）についてサイバーABに通知することを要求していません。「キャンセル」（B）はOSCの決定経路ですが、CAPは準備不足に対する適切な手続き上の対応として延期／停止を明示的に示しています。「C3PAOにガイダンスを求める」（D）は、CAPのフェーズ1準備状況判定および停止プロセスにおいて評価者／リードCCAがC3PAOに代わって行動するため、ここでは不要な表現です。

最新問題**: 71**
2人のネットワーク管理者が協力して、CMMCへの準拠に向けたネットワーク構成を決定しようとしています。しかし、いくつかの細かい点で意見が食い違うことが分かりました。CMMCへの準拠を確実にするための最適な解決策はどれでしょうか？
A. 会社のCEOに相談してください。
B. Consult the CMMC Assessment Guides and NIST SP 800-171.
C. Go with the network administrator's ideas with the least stringent controls.
D. Go with the network administrator's ideas with the most stringent controls.
Answer: B (メーッセージを残す)
When preparing forCMMC compliance, organizations must ensure that theirnetwork configurations align with required cybersecurity controls. Ifnetwork administratorsdisagree on certain configurations, the mostobjective and accurateway to resolve the disagreement is by referencingofficial CMMC guidanceandNIST SP 800-171 requirements, which form the foundation of CMMC Level 2.

Step-by-Step Breakdown:
CMMC Assessment Guides as the Primary Reference
TheCMMC Assessment Guides (Level 1 & Level 2)provide clearinterpretationsof security practices.
Theyexplain how each practice should be implemented and assessedduring certification.
NIST SP 800-171 as the Compliance Baseline
CMMC Level 2is based directly onNIST SP 800-171, which outlines the110 security controlsrequired for protectingControlled Unclassified Information (CUI).
Network configurations must complywith NIST-defined security requirements, including:
Access Control (AC) - Ensuring least privilege principles.
Audit and Accountability (AU) - Logging and monitoring network activity.
System and Communications Protection (SC) - Secure network design and encryption.
Why the Other Answer Choices Are Incorrect:
(A) Consult with the CEO of the company:
ACEO is not necessarily a cybersecurity expertand may not be familiar with CMMC technical requirements.
Technical compliance decisions should be based onCMMC and NISTframeworks, not executive opinions.
(C) Go with the network administrator's ideas with the least stringent controls:
Choosingless stringent controls increases security riskand could lead toCMMC non-compliance.
(D) Go with the network administrator's ideas with the most stringent controls:
While security is important,more stringent controlsmay introduceoperational inefficienciesorunnecessary coststhat are not required for compliance.
The correct approach is to implement what is required by CMMC and NIST SP 800-171, no more and no less.
Final Validation from CMMC Documentation:
TheCMMC Assessment GuidesandNIST SP 800-171 Rev. 2areofficial sourcesthat provide the most reliable guidance on compliance.
CMMC Level 2 is entirely based on NIST SP 800-171, making it the definitive source for resolving security disagreements.
Thus, the correct answer is:
B). Consult the CMMC Assessment Guides and NIST SP 800-171.

最新問題**: 72**
OSC（特別監視センター）が、メール本文に「CUI//SP-PRVCY//FED Only」と記載されたメールを受信した場合、この表記の意味を確認するには、どの組織のウェブサイトにアクセスすればよいでしょうか？
A. CMMC-AB
B. 国防総省請負業者向けFAQページ
C. DoD 239.7601 定義ページ

D. 奈良
Answer: D (メーッセージを残す**)**

最新問題**: 73**
評価担当者は、肯定的な意見を収集しています。これまでに、面接、実演、メール、メッセージ、プレゼンテーションなどを通じて情報を収集してきました。これらの方法は、肯定的な意見を収集する上で適切でしょうか？
A. はい、査定担当者が収集した確認事項はすべて適切であり、スクリーンショットも同様です。
B. いいえ、メールは適切な肯定の手段ではありません。
C. はい、査定員が収集した肯定的な回答はすべて適切です。
D. いいえ、メッセージを送ることは適切な肯定ではありません。
Answer: C (メーッセージを残す**)**

最新問題**: 74**
主任評価者が評価を計画し、テスト活動のスケジュールを立てています。証拠を得るためにテストを実施しなければならないのは誰ですか？
A. 中国共産党が監視する業務を通常行うOSC職員
B. 軍関係者とCCPおよび/または主任評価者が、文書化された手順の妥当性をテストする
C. 当該契約の請負業者に配属された軍関係者が、CUIの機密性を確保する。
D. 通常はその業務を行わないOSC職員が、文書化された手順の正確性を評価する。
Answer: A (メーッセージを残す**)**
CMMC評価において誰がテストを実施する必要があるかを理解するCMMCレベル2評価では、評価者は運用活動とセキュリティ対策を観察してコンプライアンスを検証する必要があります。このプロセスには以下が含まれます。
#評価の一環として、セキュリティ管理と手順をテストします。
#標準作業手順の観察により、管理が適切に実施されていることを確認します。
#現実的な評価条件を確保するため、日常的に業務を行っている運用担当者（OSC従業員）を活用する。
* 現場担当者（OSC従業員）が実際の作業を行い、評価者はそれを観察しなければならない。
* CMMC認定プロフェッショナル（CCP）または主任評価者が、テストプロセスを監督し、文書化します。
誰が検査を実施するのか？
* A. CCPが観察する通常その業務を行うOSC職員 # 正解
* CMMC評価では、実際のユーザー（OSC職員）が通常の業務を遂行する様子を評価者が観察し、セキュリティ対策を検証する必要があります。
* B. 軍関係者とCCPおよび/または主任評価者が、文書化された手順の妥当性をテストする # 不正解
* 軍関係者は、請負業者のセキュリティ管理体制のテストを行う責任を負わない。
* 評価者は観察と評価を行うが、自ら試験を実施することはない。

* C. 当該契約の請負業者に配属された軍関係者が、CUIの機密性を確保する。
# 正しくない
* 軍関係者は検査を実施しません。
* 請負業者（OSC）は、セキュリティ管理策の実施および実証に責任を負います。
* D. 通常その業務を行わないOSC職員が、文書化された手順の正確性を評価する #.偽
* 業務内容に精通していない担当者をテストに起用してはならない。
* 評価は現実世界の状況を反映していなければならないため、実際にその業務を行う従業員がそのプロセスを実演する必要がある。
正解が「A」（CCPが監視する業務を通常行うOSC職員）である理由は？
* CMMC評価プロセス（CAP）文書
* コンプライアンスを判断するためには、評価において実際の業務活動を観察する必要があることを規定する。
* CMMC-AB評価方法論
* 現実的な運用環境でのセキュリティ管理のテストが必要であり、つまり、実際のOSC職員がタスクを実行する必要がある。
* NIST SP 800-171A（NIST SP 800-171の評価手順）
* インタビューおよび観察は、当該業務を日常的に行っている担当者に対して実施すべきであることを明記する。

最新問題: **75**
企業のCMMCレベル1自己評価の範囲を決定する際、契約管理者は自社のITインフラストラクチャを管理するホスティングプロバイダーを含めます。サードパーティ組織を最も適切に表す資産タイプはどれですか？
A. ESP
B. 人々
C. 設備
D. テクノロジー
Answer: A (メーッセージを残す**)**
企業が自社のインフラストラクチャの管理に第三者のITプロバイダーを利用する場合、これらの組織はCMMCのスコープガイドラインにおいて外部サービスプロバイダー（ESP）として分類されます。
ステップごとの解説 #1. ESPとは何ですか？
* 外部サービスプロバイダー（ESP）とは、以下のサービスを提供する第三者組織です。
* ITサービス、クラウドホスティング、およびマネージドセキュリティソリューションを提供します。
* 請負業者に代わって、FCIまたはCUIを処理、保管、または送信する。
* FCIまたはCUIを取り扱う場合は、OSCと同じセキュリティ要件を満たす必要があります。

* 企業がITインフラストラクチャの管理をホスティングプロバイダーに依存している場合、そのプロバイダーはCMMCスコープガイドラインにおけるESP（エンタープライズサービスプロバイダー）に該当します。
#2. 他の選択肢が間違っている理由：
* (B) 人数
* 誤り：ESPは組織であり、個人ではありません。
* (C) 施設#
* 誤り:施設とは、オフィスビルやデータセンターなどの物理的な場所を指し、第三者サービスプロバイダーを指すものではありません。
* (D) テクノロジー#
* 誤り: ESP は技術サービスを提供しますが、CMMC におけるサードパーティ IT プロバイダーの正しい用語は「技術」ではなく ESP です。
* CMMCレベル1スコープガイドでは、外部サービスプロバイダー（ESP）を、ITインフラストラクチャおよびセキュリティサービスを管理する第三者組織と定義しています。
CMMCドキュメントからの最終検証：したがって、正解は次のとおりです。
#A. ESP（外部サービスプロバイダー）

最新問題: **76**
評価チームによる評価中に、テストまたはデモンストレーションが実施されます。OSCは、どの環境でこのテストまたはデモンストレーションを実施しなければなりませんか？
A. クライアント
B. 生産
C. 開発
D. デモンストレーション
Answer: B (メッセージを残す**)**
評価環境要件の理解
CMMCレベル2の評価において、評価者は、機密指定されていない管理情報（CUI）が取り扱われる実際の運用環境において、セキュリティ管理策が実施されていることを示す客観的な証拠を要求します。
これは、テストやデモンストレーションは、組織の実際のシステムとセキュリティ管理が使用されている本番環境で実施する必要があることを意味します。
選択肢B（生産）が正しい理由
評価チームは、セキュリティ対策が実際に適用される環境でその有効性を検証し、セキュリティ対策が実際の運用条件下で効果を発揮していることを確認する必要があります。
選択肢A（クライアント）は、「クライアント」が定義された評価環境ではないため、誤りです。
選択肢C（開発）は、開発環境でのテストは本番環境のセキュリティ状況を正確に反映しないため、誤りです。

選択肢D デモンストレーション）は誤りです。別のテスト環境でのデモンストレーションはCMMC評価の有効な証拠とはならないため、実際のセキュリティ実装は本番環境で検証する必要があります。
CMMC公式ドキュメントの参照
CMMC評価プロセス（CAP）ガイド - セクション3.5（評価方法）
NIST SP 800-171 評価手順（検証は、CUI が存在する実際のシステムで行う必要があります。）最終検証CMMC 評価では、セキュリティ コントロールを実際の運用環境で検証する必要があるため、正解はオプション B: 運用です。

有効な **CMMC-CCP** 問題集は GoShiken.com が提供された合格しやすい CMMC-CCP 試験問題集！ GoShiken.com が最新の **CMMC-CCP** 試験問題集を提供しています。GoShiken.com CMMC-CCP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CMMC-CCP 問題集をゲットする人はこちら: https://www.goshiken.com/Cyber-AB/CMMC-CCP-mondaishu.html (**23030%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **77**
組織内でFCIを含む文書を印刷するために、専用のローカルプリンタが使用されます。これはFCI資産とみなされます。プリンタがFCIに対して行う動作を最も適切に表す機能はどれですか？
A. 暗号化
B. プロセス
C. 管理
D. 配布する
Answer: B (メーッセージを残す**)**

最新問題: **78**
Which regulation allows for whistleblowers to sue on behalf of the federal government?
A. NISTSP 800-53
B. NISTSP 800-171
C. False Claims Act
D. Code of Professional Conduct
Answer: (解答を表示する**)**
Understanding the False Claims Act (FCA) and Whistleblower Protections
TheFalse Claims Act (FCA)(31 U.S.C. 3729-3733) aU.S. federal lawthat allowswhistleblowers (also known as "relators")to sue on behalf of the federal government if they believe a company issubmitting fraudulent claimsfor government funds.
The FCA includes a"qui tam" provision, which:

#Allows private individuals to file lawsuits on behalf of the U.S. government.
#Provides financial rewards to whistleblowersif the lawsuit results in recovered funds.
#Protects whistleblowers from employer retaliation.
In the context ofCMMC and cybersecurity compliance, theFCA has been used to hold companies accountableformisrepresenting their cybersecurity compliancewhen working with federal contracts.
For example:
If a companyfalsely claimscompliance withCMMC, NIST SP 800-171, or DFARS 252.204-7012butfails to meet security requirements, it could beliable under the FCA.
TheDepartment of Justice (DOJ)has pursued cases under theCyber-Fraud Initiative, using theFCA against defense contractorsfor cybersecurity noncompliance.
Thus, the correct answer isC. False Claims Actbecause it specifically allows whistleblowers tosue on behalf of the federal government.
Why the Other Answers Are Incorrect
A). NIST SP 800-53
#Incorrect.NIST SP 800-53provides security controls for federal agencies butdoes notcontain whistleblower provisions.
B). NIST SP 800-171
#Incorrect.NIST SP 800-171outlines security requirements for protectingCUI, but itdoes not have legal mechanismsfor whistleblower lawsuits.
D). Code of Professional Conduct
#Incorrect. TheCMMC Code of Professional Conductapplies toC3PAOs and assessorsbut doesnot provide a legal basis for whistleblower lawsuits.
CMMC Official References
False Claims Act (31 U.S.C. 3729-3733)- Establishes whistleblower protections and qui tam lawsuits.
DOJ Cyber-Fraud Initiative- Uses the FCA to enforce cybersecurity compliance in government contracts.
DFARS 252.204-7012 & CMMC- Require accurate reporting of cybersecurity compliance, which can lead to FCA violations if misrepresented.
Thus,option C (False Claims Act) is the correct answeras per official legal guidance.

最新問題**: 79**
CMMCレベル1自己評価の準備として、DIB組織のITマネージャーは、会社のSSPで資産の種類を文書化しています。マネージャーは、特定されたマシンコントローラーと組立機を特殊資産として文書化する必要があると判断しました。マネージャーが特定し文書化した特殊資産の種類はどれですか？
A. たくさん
B. 制限付きIS
C. 試験装置
D. 運用技術

Answer: (解答を表示する)
CMMC 自己評価における特殊資産の理解CMMC レベル 1 自己評価では、組織はシステム セキュリティ プラン (SSP) で資産を分類する必要があります。
* オペレーショナルテクノロジー（OT）には、機械制御装置、産業制御システム（ICS）、組立機械が含まれます。
これらのシステムは、製造、エネルギー、および産業環境における物理プロセスを制御します。
* OT資産は、リアルタイム制御やレガシーシステムの制約など、独自のセキュリティ上の考慮事項があるため、従来のITシステムとは異なります。
特殊資産タイプ：運用技術（OT）
* A. IoT（モノのインターネット）# 不正解
* IoTデバイスには、スマートホームシステム、接続されたセンサー、ネットワーク接続された家電製品などが含まれますが、機械制御装置や組立機械はIoTではなくOTに分類されます。
* B. 制限付き IS # 不正解
* 制限情報システム（IS）とは、機密扱いまたは高度に管理されたシステムを指し、標準的な産業機械には適用されません。
* C. 試験装置 # 不正解
* 試験装置には、品質保証に使用される診断ツールや測定装置が含まれますが、産業機械制御装置は含まれません。
* D. 運用技術 # 正解
* 機械制御装置と組立機械は、産業オートメーションおよび制御システムの一部であり、運用技術（OT）に分類されます。
正解が「D. オペレーショナルテクノロジー」である理由は？
* CMMCレベル1およびレベル2評価に関するスコープ設定ガイダンス
* 運用技術（OT）を、特別なセキュリティ上の考慮事項を必要とする特殊資産のカテゴリとして定義します。
* NIST SP 800-82（産業制御システムセキュリティガイド）
* 機械制御装置と組立機械を運用技術（OT）の一部として識別します。
* CMMC 2.0 資産分類ガイドライン
* OTシステムは組織のSSPに別途文書化する必要があることを指定します。
この回答を裏付けるCMMC 2.0の参考文献：

最新問題: **80**
評価チームのメンバーが、OSC（運用サービスセンター）に対してCMMCレベル2評価を実施しています。OSCは、AC.L1-3.1.1「情報システムへのアクセスを、承認されたユーザー、承認されたユーザーに代わって動作するプロセス、またはデバイス（他の情報システムを含む）に限定する」に基づいて評価対象を検査し、OSCから提供された証拠の妥当性を判断しています。この活動はどの評価方法に該当しますか？

A. テスト
B. 観察する
C. 検査する
D. インタビュー
Answer: (解答を表示する**)**
CMMC 2.0における評価方法の理解
CMMC評価プロセス（CAP）ガイドによると、評価者はセキュリティ対策への準拠を判断するために、主に3つの評価方法を使用します。
調査 - 文書、ポリシー、構成、およびシステム記録を確認する。
インタビュー :セキュリティプロセスに関する知見を得るために、担当者と面談する。
テスト :システム機能およびセキュリティ制御の技術的な検証を実施する。
選択肢C（調べる）が正解である理由
評価チームのメンバーは、評価オブジェクト（システム構成、ユーザーアクセス制御設定、ポリシーなど）を検査し、OSC の証拠が AC.L1-3.1.1（アクセス制御 - 承認済みユーザー）に十分であるかどうかを判断します。
この活動は、以下のような成果物をレビューする「検査方法」に直接対応しています。
アクセス制御リスト（ACL）
システムユーザー認証ログ
アカウント管理ポリシー
役割ベースのアクセス制御設定
「観察する」（選択肢B）は、CMMCにおいて「観察」は公式の評価方法ではないため、誤りです。
「テスト」（選択肢A）は、評価が実際に機能を実行するのではなく、証拠を検証するものであるため、誤りです。
「インタビュー」（選択肢D）は、職員への質問は行われず、文書の確認のみが行われているため、誤りです。
CMMC公式ドキュメントの参照
CMMC評価プロセス（CAP）ガイド、第3.5項 - 評価方法
CMMCレベル2評価ガイド - アクセス制御の実践（AC.L1-3.1.1）
最終確認
この活動は、アクセス制御措置を確認するために文書や記録を精査することを含むため、検査方法に該当し、選択肢Cが正解となります。

最新問題**: 81**
主任評価者が参照し使用すべき主要な参考資料を最も適切に説明しているのは、次のうちどれですか？
A. 国防総省が対象とする防衛情報に関する適切なセキュリティチェックリスト。
B. CMMCモデルの概要。評価方法と対象を提供します。
C. レベル2評価のためのFAR条項52.204-21に基づく安全対策要件。

D. 希望する認証レベルに対応した、公開済みのCMMC評価ガイドの実践説明。
Answer: (解答を表示する**)**
CMMC評価における主任評価者のための重要な参考資料CMMC評価を実施する主任評価者は、認証を求める組織（OSC）が要求されるサイバーセキュリティ対策を満たしているかどうかを評価するために、公式のCMMCガイダンス文書に依拠する必要があります。
CMMC評価ガイドでは、評価対象となる特定のCMMCレベルにおける各実践事項とプロセスについて詳細な説明を提供します。
これは、次のことを定義します。#各実践の評価目標。#コンプライアンスに必要な証拠。#実践が満たされているか否かを判断するための採点基準。
最も関連性の高い参考資料 :CMMC評価ガイド
A). 対象防衛情報に対する国防総省の適切なセキュリティチェックリスト # 誤り 国防総省の適切なセキュリティチェックリストは DFARS 252.204-7012 の準拠に関連していますが、CMMC の評価は CMMC 評価ガイドに従います。
B). CMMC モデルの概要は、評価方法とオブジェクトを提供するので # 誤り CMMC モデルの概要は、高レベルのガイダンスを提供しますが、具体的な評価基準は含まれていません。
C). レベル 2 評価に対する FAR 条項 52.204-21 の保護要件 # 誤り FAR 52.204-21 は CMMC レベル 1 (FCI 保護) に関連していますが、CMMC レベル 2 は NIST SP 800- に従います。
171 また、検証には CMMC 評価ガイドが必要です。
D). 希望する認証レベルに対する CMMC 評価ガイドの実践説明が公開されている # 正解 CMMC 評価ガイドは、OSC が認証に必要なセキュリティ プラクティスを満たしているかどうかを判断するために使用される公式文書です。
正解が D. 希望する認証レベルに対応した、公開されているCMMC評価ガイドの実践説明」である理由は？
CMMC評価プロセス（CAP）文書
主任評価者は、公式な採点のためにCMMC評価ガイドを使用しなければならないことを規定する。
CMMCレベル1およびレベル2評価ガイド
各実践について、詳細な説明、評価方法、および採点基準を提供します。
CMMC-AB認定第三者評価機関（C3PAO）向けガイダンスでは、CMMC評価は一般的な国防総省のセキュリティポリシーではなく、評価ガイドに従う必要があることが確認されています。
この回答を裏付けるCMMC 2.0の参考文献
最終解答 :D. 希望する認証レベルに対応する、公開されているCMMC評価ガイドの実践説明。

最新問題**: 82**

政府への製品またはサービスの開発または提供に関する契約に基づき、政府によって提供または生成される情報のうち、一般公開を目的としない情報の種類は何ですか？ただし、政府が一般に公開する情報（公共ウェブサイトなど）や、支払処理に必要な単純な取引情報は含まれません。
A. CDI
B. CTI
C. どちら
D. FCI
Answer: D (メーッセージを残す)
連邦契約情報（FCI）の理解連邦契約情報（FCI）は、48 CFR 52.204-21（対象となる契約業者情報システムの基本的保護）で定義されています。FCIとは、以下の情報を指します。
※一般公開を目的としたものではありません。
* 政府との契約に基づき、政府によって提供されるか、政府のために生成される。
政府向けに製品またはサービスを開発または提供するために必要な場合。
* 公開されている政府情報（公共ウェブサイトの情報など）は除外します。
* 単純な取引情報（例：支払処理に必要な情報）は除外します。
CMMC 2.0 のコンテキストでは、FCI を処理、保存、または送信する組織は、FAR 52.204-21 に概説されている 17 の基本的な保護対策を実施する必要がある CMMC レベル 1 (基礎) を満たす必要があります。
* A. CDI（防衛情報管理）:偽
* この用語は DFARS 252.204-7012 で使用されていましたが、CMMC の議論では CUI (管理された非機密情報) に置き換えられました。
* B. CTI（サイバー脅威インテリジェンス）:不正解
* これは、契約データではなく、サイバー脅威、戦術、および指標に関する情報を指します。
* C. CUI（管理対象非機密情報）:偽
* CUIは、追加の保護が必要な機密情報ですが、FCIとは別のカテゴリーです。
* D. FCI（連邦契約情報）:正解
* FCIの定義は、質問で示された説明と完全に一致しています。
正解がFCI（D）である理由は？
* FAR 52.204-21（対象となる請負業者の情報システムの基本的保護）
* FCIおよび必要な安全対策を定義する。
* FCI保護のための17のサイバーセキュリティ対策を確立する。
* CMMC 2.0フレームワーク
* レベル1（基礎）は、FCIを取り扱う請負業者に必須です。
* FAR 52.204-21に概説されている基本的な保護要件への準拠を保証します。
* NIST SP 800-171 および DFARS 252.204-7012
* FCIはNIST SP 800-171への準拠を要求しませんが、CUIは要求します。
この回答を裏付けるCMMC 2.0の参考文献：

最新問題: **83**

行動計画は、計画の明確な目標または目的を定義するものです。では、一般的に行動計画に含まれない情報とは何でしょうか？
A. 進捗状況を測るためのマイルストーン
B. 計画の是正措置を実施するための予算要件
C. 計画の成果を確実にする責任を負う者の所有権
D. 完了予定日
Answer: C (メーッセージを残す)

最新問題: **84**
Which term describes the prevention of damage to. protection of, and restoration of computers and electronic communications systems/services, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation?
A. Data security
B. Cybersecurity
C. Information security
D. Network security
Answer: B (メーッセージを残す)

最新問題: **85**
請負業者は、特権ユーザー向けにIA.L2-3.5.3：多要素認証のプラクティスを導入しましたが、評価中にOSCの標準ユーザーはエンドポイントやネットワークリソースへのアクセスにMFAを必要としないことが判明しました。最も適切な発見は何でしょうか？
A. プロセスは正常に実行されています。
B. これは新規取得案件のため、対象外です。
C. 新規取得は特殊資産とみなされます。
D. 目標が実施されなかったため、実践は達成されていません。
Answer: (解答を表示する)
IA.L2-3.5.3の理解：多要素認証（MFA）要件NIST SP 800-171（要件3.5.3）に基づくIA.L2-3.5.3プラクティスでは、特権ユーザーと標準ユーザーの両方が以下のものにアクセスする際に、多要素認証（MFA）を実装する必要があります。
#組織のエンドポイント（例：ノートパソコン、デスクトップパソコン、モバイルデバイス）。
#ネットワークリソース（例：VPN、内部システム）。
#管理対象非機密情報（CUI）を含むクラウドサービス。
「MET」評価の主要要件IA.L2-3.5.3を満たすためには、組織は以下の要件を満たす必要があります。
すべての特権ユーザー（システム管理者など）に多要素認証（MFA）を必須とする。
エンドポイントおよびネットワークリソースにアクセスする標準ユーザーには、多要素認証（MFA）を必須とする。
関連するすべてのシステムに多要素認証（MFA）を導入する。

OSCの現在の実装では標準ユーザーはMFAを必要としないため、この慣行は完全に実装されておらず、「未達成」と評価する必要があります。
A) プロセスは正しく実行されています #.偽
MFAは特権ユーザーにのみ適用されますが、一般ユーザーにも必須です。このプロセスはまだ完全には実装されていません。
B) これは新規買収であるため、対象外です。#.偽
新規買収案件は、CUI（機密情報またはネットワークアクセスを扱う場合、引き続きMFA（多要素認証）の要件を満たす必要があります。
C) 新規取得は特殊資産とみなされる #.偽
特殊な資産（IoT、レガシーシステムなど）には代替のセキュリティ制御が適用される場合があるが、標準ユーザーおよびエンドポイントは引き続き多要素認証（MFA）に準拠する必要がある。
D). 目標が実装されていないため、実践は達成されていません。# エンドポイントとネットワーク リソースにアクセスする特権ユーザーと標準ユーザーの両方に対して、正しいMFA を有効にする必要があります。
標準ユーザーが除外されているため、この要件は満たされていません。
正解が「D」（目標が実施されなかったため、実践は達成されていない）である理由は？
CMMC 2.0 レベル2（上級）要件
CUIおよびネットワークリソースにアクセスするすべてのユーザーにMFAを適用する必要があることを指定します。
NIST SP 800-171（要件3.5.3 - MFAの実装）
特権ユーザーおよび一般ユーザーを含む、すべてのユーザータイプに対して多要素認証（MFA）を必須とします。
CMMC評価プロセス（CAP）文書
METとみなされるためには、実践が完全に実施されている必要があると規定している。部分的な実施は、METではないことを意味する。
この回答を裏付けるCMMC 2.0の参考文献。

最新問題: **86**
主任評価者がCMMC準備状況レビューを実施しています。主任評価者は既に評価リスク状況と全体的な評価の実現可能性を記録しています。最低限、残りの準備状況レビュー基準のうち、検証すべき項目は何ですか？
A. ロジスティクス、評価チーム、および証拠の準備状況を決定する。
B. 初期モデル実践評価を決定し、記録する。
C. 予備的な推奨所見を決定する。
D. 練習の合否結果を判定します。
Answer: A (メーッセージを残す**)**

最新問題: **87**

国防総省由来または国防総省向けの旧来のマーキングが施されたデータや文書は、どのような場合に再マーキングまたは編集が必要となるのでしょうか？
A. 国防総省の管理下にある場合
B. 文書が機密とみなされる場合
C. 組織外に文書を共有する場合
D. 派生文書の元の情報がCUIでない場合
Answer: C (メーッセージを残す)
レガシーマーキングとCUIに関する背景情報
旧来のマーキングとは、国防総省指令5200.48に基づく管理対象非機密情報（CUI）プログラムの実施前に使用されていた分類ラベルを指します。
従来の表示（公務専用」（FOUO）や「機密だが非機密」（SBU）など）が付いた文書は、CUIの要件に合わせるために、表示の変更または編集について見直す必要があります。
旧式の標識はいつ更新する必要があるのか？
文書が内部的に保管される場合（回答A - 不正解）：国防総省の管理下にある文書は、外部に共有されない限り、直ちに再マーキングする必要はありません。
文書が機密扱いの場合（回答B - 不正解）この質問は機密情報ではなく、CUI に関するものです。機密レベルの文書は、国防総省マニュアル 5200.01 に基づく異なるマーキング規則に従います。
ドキュメントが外部に共有されている場合（回答C - 正解）：
国防総省指令5200.48、第3.6項(a)によれば、組織は組織外に文書を共有する前に、過去の記録を精査しなければならない。
当該文書は、配布前にCUIプログラムに準拠して再マークされなければならない。
元の文書に CUI が含まれていない場合 (回答 D - 不正解): 元のソース文書の状態は、派生文書に CUI が含まれている場合に、派生文書を再マークする要件には影響しません。
結論
正解はCです。旧来のマークが付いた文書は、組織外で共有する際に、国防総省のCUIガイドラインに準拠するために、マークを付け直すか、編集する必要があります。
国防総省指令5200.48（機密解除された管理情報）
米国国立公文書館（NARA）によるCUIマーキングハンドブック、CUI環境向けCMMC 2.0スコープガイド

最新問題: **88**
評価チームが、文書化され毎月チェックされている業務手順を審査しています。ログを確認したところ、その業務手順は四半期ごとにしか実施されていないことが判明しました。面談で、チームメンバーは業務手順は毎月実施しているが、文書化は四半期ごとだと説明しました。この状況で、業務手順の合格基準を満たすことができるでしょうか？
A. いいえ、作業は記載どおりには行われていません。
B. はい、手順は文書に記載されているとおりに実施されています。
C. いいえ、合格するには3つの評価方法すべてを満たす必要があります。

D. はい。面接プロセスは練習に合格するのに十分です。
Answer: C (メーッセージを残す)
CMMC評価要件の理解
* CMMC評価では、セキュリティ対策への準拠を確認するために3つの評価方法を使用します。
* 調査 - 文書、ポリシー、ログ、または記録を確認する。
* インタビュー - 担当者と話をして、理解度と実行状況を確認する。
* テスト - 技術的または運用上の手段によって、その手順が実行されていることを確認すること。
提示されたシナリオにおける評価結果
* 練習は毎月実施されていると記録されているが、ログには四半期ごとの実施が示されている。
* インタビューでは月次で実施されているとされているが、文書ではこの主張を裏付けていない。
組織が実践に失敗する理由
* 回答 A (不正解): 作業は実行されているが、ドキュメントが不足しているため、失敗は実行不足だけが原因ではない。
* 回答 B（不正解）：記録された頻度がログの証拠と一致しないため、手順は完全に記録されたとおりに実行されていません。
* 回答C（正解）CMMCでは、3つの評価方法（調査 インタビュー、テスト）すべてが一致している必要があります。ログに記載されている頻度と矛盾するため、この方法は準拠していません。
* 回答 D (不正解): インタビューでの回答だけでは不十分です。CMMCCAP ガイドおよび NIST SP 800-171 では、ログ (調査) と技術的検証 (テスト) による裏付けが必要です。
結論
* 正解はCです。組織が実務に合格するには、3つの評価方法すべてにわたる証拠を提出する必要があります。
:
CMMC評価プロセス（CAP）ガイド - Cyber AB
NIST SP 800-171A - CUIのセキュリティ要件の評価
DoD CMMC 2.0 スコープ設定および評価ガイド

最新問題**: 89**
SI.L2-3.14.7: 組織システムの不正使用の特定は、2 つの評価目標を使用して評価されます。評価目標は、システムの正規使用が定義されているかどうか、およびシステムの不正使用が特定されているかどうかを判断することです。この実践に対する最良の証拠は何ですか?
A. リスク対応
B. リスク評価
C. インシデント対応
D. システム監視

Answer: D (メーッセージを残す)
SI.L2-3.14.7（不正使用の特定）の評価目標は、次の2つの成果に焦点を当てています。(a) 組織がシステムの正規使用を定義していること、(b) 組織が不正使用が発生した際にそれを特定できること。したがって、最も有力な証拠は、組織がシステムを積極的に監視し、定義された正規使用の基準範囲外の活動を検知および認識できることを示す証拠です。
DoD CMMC評価ガイド - レベル2（v2.13）のSI.L2-3.14.7の「潜在的な評価方法と対象」では、継続的な監視戦略、システムおよび情報整合性ポリシー、システム監視ツールと技術に関する手順、技術的な監視機能（IDS/IPSなどのツール/技術）など、監視と検出に直接関連する成果物が強調されています。
（監査記録の監視、ネットワーク監視など）。
これらの成果物は、不正使用が実際に特定されていること（アラート、ログ、相関関係、レビュープロセス）と、許可された使用が定義されていること（何が許可されているかを確立するポリシー/標準）をまさに証明するものです。
「承認済み」は「承認されていない」と区別できるように表示されている。
対照的に、リスク評価／対応とインシデント対応は関連するプログラム要素ではありますが、組織が不正使用を継続的に検知していることを示す主要な証拠ではありません。評価ガイドは監視対象に重点を置いているため、システム監視が最良の証拠となります。

最新問題: **90**
CMMCアセスメントの実施中に、OSCの担当者がアセスメント担当者にレビュー用の文書を提供します。この文書には、インシデント対応能力が確立されていること、およびインシデントの準備、検出、分析、封じ込め、復旧、ユーザー対応活動に関する情報が記載されています。この文書は、どのCMMCプラクティスを証明しているのでしょうか？
A. IR.L2-3.6.1: インシデント対応
B. IR.L2-3.6.2: インシデント報告
C. IR.L2-3.6.3: インシデント対応テスト
D. IR.L2-3.6.4: 流出事故
Answer: A (メーッセージを残す)
CMMC 2.0インシデント対応の実践方法を理解する
CMMC 2.0 レベル 2 のインシデント対応 (IR) ドメインは、インシデント対応能力を確立および維持するための要件を定義する NIST SP 800-171 のセクション 3.6 に準拠しています。
「A. IR.L2-3.6.1: インシデント対応」が正しい理由は？
提供された文書には、準備、検出、分析、封じ込め、復旧、およびユーザー対応活動を含むインシデント対応機能について説明されています。
IR.L2-3.6.1では、組織に対し、以下の事項を網羅するインシデント処理プロセスを確立することを具体的に要求しています。
準備
検出と分析

封じ込め
根絶と回復
事後対応
他の回答が間違っている理由とは？
B). IR.L2-3.6.2 :インシデント報告（誤り）
インシデント報告は、外部機関（例：国防総省DIBNet）へのインシデント報告に重点を置いており、提供されたドキュメントの説明とは異なります。
C). IR.L2-3.6.3: インシデント対応テスト（不正解）
インシデント対応テストは、対応プロセスが定期的にテストおよび評価されることを保証するものであり、提供されるドキュメントの主な焦点ではありません。
D)。IR.L2-3.6.4: 流出事件 (誤)
インシデント漏洩とは、具体的にはCUIへの曝露、または許可されていないCUIの取り扱いに関するインシデントを指し、これはここで説明されているシナリオとは異なります。
結論
正解はAです。IR.L2-3.6.1 :インシデント処理。文書にはインシデント対応能力の確立が明記されています。
参考文献：
CMMC 2.0 レベル2の実施基準（NIST SP 800-171、セクション3.6）
CMMC評価プロセス（CAP）ガイド

最新問題**: 91**
評価担当者は、OSCの担当者と協力して、今後の評価の計画と準備を進めています。評価の要件を分析する際に、最も重要なことの一つは何でしょうか？
A. 評価の範囲設定は簡単で、心配もいりません。
B. 当初の計画は、一度合意されると変更できません。
C. OSCの連絡担当者が証拠と概算額を提出できる期限が定められています。
D. 評価者は、情報が集まるにつれて、評価の要件と計画を継続的に見直し、更新する必要があります。
Answer: (解答を表示する**)**
CMMC評価の計画と準備には、評価者と認証取得希望組織（OSC）との連携が不可欠であり、評価範囲、必要な証拠、およびロジスティクスを決定する必要があります。この計画プロセスは動的であり、新たな情報が得られるにつれて適応していく必要があります。
正解が「D」である理由は？
評価範囲および要件は変更される場合があります
評価担当者が証拠を収集し、環境を分析する過程で、資産、ネットワーク、セキュリティ管理に関する新たな詳細情報が得られた場合、評価計画の調整が必要になる可能性があります。
CMMC評価プロセス（CAP）ガイドでは、評価要件と範囲は、リアルタイムの調査結果を反映させるために継続的に見直し、更新する必要があることを強調しています。
評価者は適応的なアプローチを採用する

CMMC評価の過程で、組織は追加のFCIまたはCUI資産を発見する可能性があり、それによって評価対象となるセキュリティ対策が変更される場合があります。
評価者は、当初の不変の計画に厳密に従うのではなく、状況に応じて評価方法を見直すべきである。
他の選択肢を選ばない理由は？
A) 評価範囲の設定は簡単で心配無用です#不正解
スコープ設定は、OSCの情報システムと資産を慎重に評価する必要がある、重要かつ複雑なプロセスです。
CMMCスコープ設定ガイドでは、対象となる資産を特定することは非常に重要であり、相当な労力を要すると述べている。
B) 合意された当初の計画は変更できない.偽
初期評価計画は出発点に過ぎず、リアルタイムの調査結果に基づいて柔軟に対応できるものでなければならない。
CMMC CAPガイドは、評価プロセスにおける継続的な改善を重視しています。
C) OSCの担当者が証拠を提出する期限と大まかな目安が定められています。#誤り 期限はありますが、重要な焦点は、厳密な期限に間に合うように急ぐのではなく、必要なすべての証拠が正確に収集されていることを確認することです。
関連するCMMC 2.0の参考文献：
CMMC評価プロセス（CAP）ガイドでは、追加情報が収集されるにつれて、評価要件と計画を更新する必要があると規定されています。
CMMCスコープ設定ガイド（2021年11月）- 評価者は、プロセス全体を通して、スコープ内の資産と要件を継続的に精査する必要があることを説明しています。
最終的な正当化：
評価計画は動的なプロセスです。評価者は、新しい情報が現れたら要件と計画を継続的に見直し、更新する必要があります。Dが正解です。

有効な **CMMC-CCP** 問題集は GoShiken.com が提供された合格しやすい CMMC-CCP 試験問題集！ GoShiken.com が最新の **CMMC-CCP** 試験問題集を提供しています。GoShiken.com CMMC-CCP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CMMC-CCP 問題集をゲットする人はこちら: https://www.goshiken.com/Cyber-AB/CMMC-CCP-mondaishu.html (**23030%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **92**
情報提供依頼書および提案依頼書において、必要なCMMCレベルを指定するのはどの組織ですか？
A. 国防総省
B. 奈良

C. NIST
D. 国土安全保障省
Answer: A (メーッセージを残す)
* 米国国防総省（DoD）は、契約に関わる情報の機密性に基づいて、必要なCMMCレベルを決定します。
* 必要なCMMCレベルは、情報提供依頼書（RFI）および提案依頼書（RFP）に明記されています。
参照：
DFARS 252.204-7021（CMMC要件）
CMMC 2.0 プログラムドキュメント
ステップ2：他の選択肢が間違っている理由B. NARA（不正解）：
米国国立公文書館（NARA）はCUIプログラムの方針を監督するが、CMMCレベルを割り当てる権限はない。
C: NIST (不正解):
米国国立標準技術研究所（NIST）はサイバーセキュリティフレームワーク（例NIST SP）を開発しています。
800-171）だが、契約書にCMMCレベルを明記していない。
D：国土安全保障省（誤）：
国土安全保障省（DHS）は国家レベルでのサイバーセキュリティを担当していますが、CMMCは特に国防総省の請負業者に適用されます。
正解の最終確認：国防総省は、RFIおよびRFPにおいて必要なCMMCレベルを決定し、規定します。

最新問題**: 93**
C3PAOはOSCのレベル2評価をほぼ完了しました。CMMC調査結果概要とCMMC評価結果文書は既に作成済みです。最終推奨評価結果が現在作成中です。これらの結果を作成する際に、必ず含めなければならないものは何ですか？
A. 更新された評価計画
B. 記録され、最終更新されたデイリーチェックポイント
C. C3PAOとOSCの間で締結されたCMMC評価契約が完全に履行されました。
D. CMMC品質保証プロフェッショナル（CQAP）のドキュメントを確認する
Answer: D (メーッセージを残す)
CMMC評価プロセス（CAP）によれば、特にフェーズ4：結果報告の要件において、C3PAOは、すべての評価パッケージが最終化され国防総省（DoD）に提出される前に、厳格な品質レビューを受けることを保証しなければならない。
CQAPの役割：CMMC品質保証専門家（CQAP）は、C3PAO内の指定された役割であり、評価がCAPに従って実施されたこと、および収集された証拠（「アーティファクト」）が調査結果（達成/未達成）を裏付けていることを検証する責任を負います。

必須事項：最終推奨評価結果を作成する際、CQAPからの正式なレビュー文書がなければ、パッケージは完全または有効とはみなされません。この文書は、C3PAOの内部品質管理システム（QMS）が評価チームの作業を検証したことを示す「承認印」となります。
他の選択肢が間違っている理由：
オプションA：評価計画は計画段階で必須の文書ですが、品質検証と同様に最終結果生成の必須コンポーネントではなく、プロセスへのインプットです。
オプションB：日々のチェックポイントは、「評価の実施」フェーズ中にOSCに情報を提供するために使用される管理ツールです。これらは評価記録の一部ではありますが、最終結果パッケージの必須の技術的構成要素ではありません。
オプションC：契約は「計画と準備」フェーズで処理される法的/ビジネス上の要件であり、国防総省にアップロードされる技術評価結果には含まれません。
参考資料：
CMMC評価プロセス（CAP）v1.0：セクション4.2（評価レポートの最終化）およびセクション4.3（C3PAO品質レビュー）。
C3PAO認証要件：エコシステム全体における一貫性と完全性を確保するため、すべての評価結果をレビューする品質保証（QA）機能が必要であることを規定します。

最新問題: **94**
FAR条項52.204-21の目的を最も適切に説明しているのはどれですか？
A. この条項に記載されているサイバーセキュリティシステムを設置するよう、対象となるすべての請負業者に指示しています。
B. 対象となる請負業者ISを保護するために請負業者が講じなければならないすべての安全対策について説明します。
C. これは、請負業者が対象となる請負業者ISを確保するために取らなければならない最低限の注意基準を説明しています。
D. 対象となる請負業者に対し、契約の最低要件と同等のレベルのCMMC認証を取得するよう指示する。
Answer: C (メーッセージを残す**)**
FAR条項52.204-21の理解連邦調達規則（FAR）条項52.204-21は「対象となる請負業者情報システムの基本的な保護」と題されています。この条項は、連邦契約情報（FCI）を扱う連邦政府請負業者に対する最低限のサイバーセキュリティ要件を定めています。
FAR条項52.204-21の主な目的FAR 52.204-21の主な目的は、請負業者がFCIを処理、保存、または送信する情報システムに基本的なサイバーセキュリティ保護を適用することを保証することです。
これらの最低限の安全対策要件は、米国政府と取引を行う請負業者にとっての基本的なセキュリティ基準として機能する。
* FAR 52.204-21では、請負業者に特定のサイバーセキュリティツールをインストールすることを義務付けていません（オプションAは除外されます）。

* これは、完全なセキュリティに必要なすべてのサイバーセキュリティ対策ではなく、最低限の安全対策のみを概説しています（オプションBを排除）。
* この条項のみではCMMC認証は義務付けられていません（オプションDは除外されます）。
* その代わりに、FCIを保護するためにすべての連邦政府契約業者が従わなければならない基本的な「注意基準」を確立します（したがって、選択肢Cが正解です）。
「最低限のケア基準」が正しい理由は何ですか？回答の選択肢の内訳オプションの説明正しいですか？
A :この条項は、対象となるすべての請負業者に対し、当該条項に記載されているサイバーセキュリティシステムを設置するよう指示しています。
#誤り - この条項ではツールを指定したり、特定のサイバーセキュリティシステムを要求したりしていません。
B :これは、請負業者が対象となる請負業者情報システム（IS）を保護するために講じなければならないすべての安全対策について説明しています。
#誤り - これは最低限の要件のみを設定しており、可能なすべてのセキュリティ対策を設定しているわけではありません。
C :これは、請負業者が対象となる請負業者ISを確保するために取るべき最低限の注意基準を説明するものです。
#正しい - この条項は、基本的な安全対策を最低限のセキュリティ基準として定義しています。
D. 対象となる請負業者に対し、契約で定められた最低要件と同等のレベルのCMMC認証を取得するよう指示する。
#誤り - FAR 52.204-21はCMMC認証を義務付けていません。その要件はDFARSによるものです。
252.204-7012および7021。
FAR 52.204-21に基づく最低限のセキュリティ要件 この条項では、CMMCレベル1に準拠した15の基本的なセキュリティ管理策を定義しています。例としては、以下のものがあります。
#アクセス制御 - 許可されたユーザーのみにアクセスを制限します。
#識別と認証 - システムユーザーを認証します。
#メディア保護 - 廃棄前にメディアを消毒してください。
#システムおよび通信保護 - ネットワーク接続を監視および制御します。
* FAR 52.204-21 - FCI の基本的な安全対策要件を定めます。
* CMMC 2.0 レベル 1 - FAR 52.204-21 の管理策に直接準拠しています。
CMMC 2.0 および FAR 文書からの公式参照最終検証と結論正解は C です。これは、請負業者が対象となる請負業者 IS を保護するために取るべき最低限の注意基準を説明しています。これは、FCI のベースライン セキュリティ基準として FAR 52.204-21 の要件と一致します。

最新問題: **95**

評価者の証拠収集活動を最も適切に説明しているのは、次のうちどれですか？
A. レベル2の実践を評価するためにインタビューを使用する。
B. レベル2の実践に関するすべての実践または目標をテストする
C. 特定の評価目標をテストして結果を判断する。
D. 十分な証拠を集めるために、検査、面接、テストを実施する。
Answer: D (メーッセージを残す)
CMMC評価プロセス（CAP）およびCMMC 2.0ガイドラインに基づき、評価者は組織が要求されるセキュリティ対策とプロセスを満たしていることを検証するために、客観的な証拠を収集する必要があります。この証拠収集は、主に次の3つの評価方法によって行われます。
* 調査 - 文書、記録、システム構成、その他の成果物のレビュー。
* インタビュー - 担当者と話をして、プロセス、責任、およびセキュリティ管理に関する理解を確認する。
* テスト - システムの動作を観察し、技術的な検証を行い、リアルタイムで制御を実行して有効性を検証します。
* CMMC評価プロセス（CAP）では、評価者はコンプライアンスを判断するために、証拠収集方法（検査、インタビュー、テスト）を組み合わせて使用する必要があると規定されています。
* CMMC 2.0 レベル 2 (NIST SP 800-171 に準拠) では、評価者はポリシーと手順が存在するだけでなく、それらが実装され、効果的であることも検証する必要があります。
* （オプションAのインタビューのような）1つの方法だけに頼るのは不十分です。
* すべての実践または目標をテストする（オプションB）必要はありません。評価者は、どの目標をより詳細に調査する必要があるかを判断するために、範囲に関するガイダンスに従います。
* 「特定の」目標のみをテストする（オプションC）ことは、複数の方法から十分な証拠を収集するという要件に完全には合致しません。
* CMMC評価プロセス（CAP）ガイドのセクション3.5 - 評価方法では、試験、面接、テストの使用が効果的な評価の基礎であると明確に定義されています。
* CMMC 2.0 レベル 2 プラクティスおよび NIST SP 800-171 では、評価者がセキュリティ制御の存在、実装、および有効性を検証することが求められています。
* CMMC付録E：評価手順では、評価者はコンプライアンスを判断するために複数の証拠源を使用すべきであると規定されています。
オプション D が正解である理由 CMMC 2.0 および公式文書の参照 最終検証 CMMC 2.0 ガイドラインおよび公式文書への準拠を確保するため、評価者は検査、インタビュー、テストを使用して効果的に証拠を収集する必要があります。そのため、オプション D が正解となります。

最新問題: **96**

OSC（オンタリオ州証券委員会）のレベル2評価が終盤を迎え、最終結果をOSCに提出するための準備が進められています。最終結果はいつOSCに提出すべきでしょうか？
A. 評価の毎日の終わりに
B. 毎日および最終の別日程のレビュー時に
C. 最終日次チェックポイント時、または別途予定されている所見および推奨事項のレビュー時
D. C3PAOの承認後、または別途予定されている最終勧告事項レビューの期間中。
Answer: (解答を表示する**)**
CMMC 2.0 レベル 2 アセスメントにおける報告プロセスの理解 認定第三者評価機関 (C3PAO) が実施する CMMC レベル 2 アセスメントは、証拠の収集、コンプライアンスの評価、および認証取得組織 (OSC) への結果報告について、構造化されたアプローチに従います。報告プロセスは、CMMC アセスメント プロセス (CAP) ガイドに概説されており、結果の伝達方法が規定されています。
* 毎日のチェックポイント：
* 評価期間中、評価チームはOSCと毎日チェックポイント会議を開催し、進捗状況、観察事項、および予備的な調査結果について最新情報を提供する。
* これらのチェックポイントは透明性を確保し、OSCが軽微な問題が発生した場合に対処できるようにするものです。
* 最終結果の発表:
最終評価結果は通常、毎日の最終チェックポイントで共有されるか、または別途スケジュールされた所見と推奨事項のレビュー会議で共有されます。
* これにより、公式報告書が提出される前に、OSC（オンタリオ州検察庁）が評価結果の構造化された完全な要約を受け取ることが保証されます。
* CMMC評価プロセス（CAP）ガイドのセクション4.5では、評価結果は最終日次チェックポイントまたは別途スケジュールされた最終レビューのいずれかで提示されるべきであると明確に述べられています。
* これは、透明性を維持し、最終報告書の提出前にOSCが評価結果を明確に把握できるようにするためのベストプラクティスに沿ったものです。
* オプションA（毎日終了時は誤りです。評価者は最新情報を提供しますが、毎日「最終結果」を提供するわけではありません。
* オプション B (毎日と別途の最終レビュー) は誤解を招く表現です。CAP ガイドでは、評価者は毎日の最終チェックポイントまたは別途の所見レビューのいずれかを選択でき、両方を選択することはできません。
* オプションD（C3PAOの承認後）は誤りです。C3PAOは、調査結果がOSCに伝達される前に承認を行うことはありません。評価チームが最初に直接結果を提示します。
* CMMC評価プロセス（CAP）ガイド、セクション4.5：報告と結果の伝達
* CMMC 2.0 レベル2評価プロセスの概要
* CMMC評価最終報告書ガイドライン

評価コミュニケーション構造オプションCが正しい理由公式CMMCドキュメント参照最終検証公式CMMC 2.0ドキュメントに基づくと、最終評価結果は、毎日の最終チェックポイントまたは別途スケジュールされたレビューセッションでOSCに提示される必要があり、オプションCが正解となります。

最新問題: **97**
組織システムの範囲を定める際、サイバーセキュリティCUIプラクティスの適用範囲は、以下のコンポーネントに適用されます。
A. CUIを処理、保存、または送信する連邦システム。
B. CUIを処理、保存、または送信する非連邦システム。
C. CUIを処理、保存、または送信する連邦システム、またはシステムコンポーネントを保護するシステム。
D. CUIを処理、保存、または送信する非連邦システム、またはシステムコンポーネントを保護するシステム。
Answer: D (メーッセージを残す)
CMMC 2.0フレームワークは、CUIを処理、保存、または送信する非連邦システムに適用されます。
スコープ設定によって、どのシステムコンポーネントがCMMCの基準に準拠する必要があるかが決定されます。
システムがCUI（機密情報を処理、保存、または送信する場合、あるいはこれらのシステムのセキュリティを提供する場合は、評価範囲に含める必要があります。
CMMCは請負業者に適用され、連邦政府のシステムには適用されない。
CMMCは、国防総省（DoD）の請負業者向けに設計されており、連邦政府のシステム向けではありません。
連邦政府のシステムは既にNIST SP 800-53およびその他の規制によって管理されている。
対象範囲には、CUIを処理するシステムと、それらを保護するシステムの両方が含まれます。
CUIを処理、保存、または送信するシステムは対象範囲に含まれる。
CUIシステムを保護するシステム（ファイアウォール、監視ツール、セキュリティ機器など）も対象範囲に含まれます。
A) CUIを処理、保存、または送信する連邦システム。#不正解
CMMCは連邦政府システムには適用されません。
B) CUIを処理、保存、または送信する非連邦システム。#部分的に正しいが不完全。CUI資産を保護するセキュリティシステムは除外されているが、それらも対象に含まれる。
C) CUIを処理、保存、または送信する連邦システム、またはシステムコンポーネントを保護する連邦システム。
#正しくない
CMMCは連邦政府以外のシステムにのみ適用されます。

CMMCスコープガイド（2021年11月）- CMMCがCUIを処理する非連邦システムにも適用されることを確認します。
NIST SP 800-171 Rev. 2 - CUIを扱う非連邦システムのセキュリティ要件を規定します。
DFARS 252.204-7012 - 国防総省の請負業者に対し、CUIを扱う非連邦システムでNIST SP 800-171を実施することを義務付けています。
CMMC 2.0 のスコープの理解正解が D. CUI を処理、保存、または送信する非連邦システム、またはシステム コンポーネントを保護するシステム」である理由?他のオプションではない理由?関連する CMMC 2.0 の参照:最終的な正当化:CMMC は、CUI を処理する非連邦システム、またはそれらのシステムを保護する非連邦システムに適用されるため、正解は D. CUI を処理、保存、または送信する非連邦システム、またはシステム コンポーネントを保護するシステムです。

最新問題**: 98**
組織が非必須プログラムの使用を制限、無効化、または防止することを義務付ける慣行がある分野はどれですか？
A. アクセス制御（AC）
B. メディア保護（MP）
C. 資産運用（AM）
D. 構成管理（CM）
Answer: (解答を表示する**)**
CMMC 2.0における構成管理（CM）の役割を理解する
CMMC 2.0の構成管理（CM）ドメインは、脆弱性を引き起こす可能性のある不正な変更や不要な変更を防止するために、システムが安全に構成および維持されることを保証します。CMにおける重要な要件の1つは、セキュリティリスクを軽減するために、重要でないプログラムの使用を制限、無効化、または防止することです。
関連するCMMC 2.0の実践例：
CM.L2-3.4.1 - 組織システムで使用される情報技術製品のセキュリティ構成設定を確立し、適用する。
この慣行では、組織はシステム構成を管理し、攻撃対象領域を縮小するために、不要なプログラム、機能、ポート、およびサービスを削除または制限することが求められます。
目標は、システム上で必要かつ承認されたソフトウェアのみが実行されるようにすることで、サイバー脅威への曝露を最小限に抑えることです。
正解がCM（D）である理由は？
A). アクセス制御（AC）# 不正解
アクセス制御（AC）は、プログラムの制限ではなく、システムやデータに対するユーザーの権限とアクセスを管理することに重点を置いています。
B). メディア保護 (MP) # 不正解
メディア保護（MP）は、ソフトウェアやシステム構成ではなく、リムーバブルメディア（USBメモリ、ハードドライブなど）の保護と制御を扱います。

C). 資産管理 (AM)# 不正解
資産管理 (AM)とは、IT資産を識別し追跡することであり、ソフトウェアの設定や制限を行うことではない。
D). 構成管理 (CM) # 正解
CMは、不要なプログラム、ポート、サービス、および機能を制限することによってシステム構成を保護することを明確に規定しているため、これが正解です。
この回答を裏付けるCMMC 2.0の参考文献：
CMMC 2.0 実践 CM.L2-3.4.1 (セキュリティ構成管理)
システムを保護するために、組織はセキュリティ構成設定を遵守し、不要なプログラムを削除することが求められる。
NIST SP 800-171 要件 3.4.1
セキュリティリスクを防止するため、安全な構成設定をサポートし、不正なアプリケーションを制限します。
CMMC 2.0 レベル2要件
この慣行はレベル2（上級の要件であり、機密指定されていない管理情報 (CUI)を取り扱う組織はこれに従わなければなりません。

最新問題: **99**
CUI（機密情報を含む物理的またはデジタル資産を扱うために必要な要件を参照するドメインはどれですか？
A. メディア保護 (MP)
B. 物理的保護 (PE)
C. システムおよび情報インテグリティ (SI)
D. システムおよび通信保護 (SC)
Answer: (解答を表示する**)**
メディア保護 (MP) 領域の理解
CMMC 2.0のメディア保護 (MP)ドメインは、管理対象非機密情報 (CUI)を含む物理的またはデジタルメディアを扱うために必要なセキュリティ要件に焦点を当てています。
このドメインには以下の制御が含まれます。
CUI（機密情報を保存するデジタルメディアおよび物理メディアを保護する。
廃棄または再利用前に、メディアを消毒および破壊する。
CUIメディアへのアクセスを許可された担当者のみに制限する。
正解が "A. メディア保護 (MP)"である理由は？
MPドメインは、暗号化、アクセス制御、保管、廃棄など、CUIメディアの取り扱いに関する要件に直接対応します。
CMMC 2.0レベル2は、CUIを含むメディアを管理するためのMPコントロールを含むNIST SP 800-171に準拠しています。
他の選択肢を選ばない理由は？
B). 物理的保護 (PE)#不正解

PEは、物理的なセキュリティ（例：施設のアクセス、訪問者ログ、物理的な障壁）に焦点を当てており、メディア上のCUIの取り扱いには焦点を当てていません。
C). システムおよび情報インテグリティ（SI）#不正解
システム監視、脆弱性管理、インシデント対応に関するアイデアであり、メディア保護に関するアイデアではありません。
D). システムおよび通信保護（SC）#不正解
SCはネットワークセキュリティ、暗号化、安全な通信を扱いますが、メディア処理には特化していません。
関連するCMMC 2.0の参考文献：
CMMC レベル 2 プラクティス MP.3.125 - CUI を含むメディアの適切な取り扱いを確保することにより、CUI を保護します。
NIST SP 800-171 (MPファミリー) - CUIを含むデジタルおよび物理メディアの取り扱いに関するセキュリティ要件を規定する。
CMMCスコープガイド（2021年11月）- MPコントロールがCUIを保存、処理、または送信するすべてのメディアに適用されることを確認します。
最終的な正当化：
メディア保護（MP）はCUIを含む資産の取り扱いを直接扱うため、正解はAです。
メディア保護（MP）。

最新問題**: 100**
What is the primary intent of the verify evidence and record gaps activity?
A. Map test and demonstration responses to CMMC practices.
B. Conduct interviews to test process implementation knowledge.
C. Determine the one-to-one relationship between a practice and an assessment object.
D. Identify and describe differences between what the Assessment Team required and the evidence collected.
Answer: D (メーッセージを残す**)**
Understanding the "Verify Evidence and Record Gaps" Activity in a CMMC Assessment
During aCMMC Level 2 Assessment, theAssessment Teamfollows a structured methodology toverify evidenceand determine whether theOrganization Seeking Certification (OSC)has met all required practices.
One of the key activities in this process is"Verify Evidence and Record Gaps", which ensures that the assessment findings accurately reflect any missing or inadequate compliance evidence.
Step-by-Step Breakdown:
#1. Primary Intent: Identifying Gaps Between Required and Collected Evidence
TheAssessment Teamcompares the evidence provided by the OSC against theCMMC practice requirements.
If evidence ismissing, insufficient, or inconsistent, assessors mustdocument the gapand describe what is lacking.

This ensures that compliance deficiencies are clearly identified, allowing the OSC to understand what must be corrected.
#2. How This Process Works in a CMMC Assessment
Assessorsreview collected documentation, system configurations, policies, and interview responses.
They verify that the evidencematches the expected implementationof a practice.
If gaps exist, they arerecordedfor discussion and potential remediation before assessment completion.
#3. Why the Other Answer Choices Are Incorrect:
(A) Map test and demonstration responses to CMMC practices.#
Incorrect:While mapping evidence to CMMC practices is part of the assessment, theprimary intentof the
"Verify Evidence and Record Gaps" step is toidentify deficiencies, not just mapping responses.
(B) Conduct interviews to test process implementation knowledge.#
Incorrect:Interviews are a method used during evidence collection, but they arenot the primary focusof the verification and gap analysis step.
(C) Determine the one-to-one relationship between a practice and an assessment object.#
Incorrect:The assessment teamreviews multiple sources of evidencefor each practice, and some practices require multiple assessment objects. The goal isnot a strict one-to-one mappingbut rathera holistic validation of compliance.
Final Validation from CMMC Documentation:
CMMC評価プロセスガイドでは、「証拠の検証とギャップの記録」は、評価者が期待される証拠と提出された証拠を比較し、不一致を文書化するステップであると規定されています。これにより、評価結果と是正計画の透明性が確保されます。
したがって、正解は次のとおりです。
D) 評価チームが要求した内容と収集した証拠との間の相違点を特定し、説明する。

最新問題**: 101**
OSC（特別支援教育の評価計画を作成する際の最後のステップは何ですか？
A. 必要に応じて評価計画とスケジュールを更新する
B. 認証評価準備状況レビューを実施する。
C. 評価を実施する準備ができていることを確認する。
D. 評価計画へのコミットメントを取得し、記録する。
Answer: D (メーッセージを残す**)**

最新問題**: 102**
ある企業には、政府サービス部門と商業サービス部門があります。政府サービス部門は連邦政府の顧客のみを対象とし、定期的にFCI（連邦政府情報を受け取ります。商業サービス部門は連邦政府以外の顧客のみを対象とし、公開されている情報のみを処理します。この

企業のCMMCレベル1自己評価において、商業サービス部門を支える資産はどのように分類すべきでしょうか？
A. FCIアセット
B. 特殊資産
C. 対象外資産
D. 運用技術資産
Answer: C (メーッセージを残す)
CMMC資産分類の理解
CMMC 2.0 スコープガイドでは、資産が連邦契約情報 (FCI) および管理対象非機密情報 (CUI) に関与しているかどうかに基づいて、資産をどのように分類するかを定義しています。
このシナリオでは：
政府サービス部門は連邦政府の顧客とやり取りし、FCI（財務コンプライアンス情報）を受け取るため、その資産はCMMCレベル1の対象となります。
商業サービス部門は連邦政府以外の顧客とのみやり取りを行い、FCI（連邦通信インフラ）を取り扱いません。つまり、その資産はCMMCレベル1の要件の対象ではなく、対象外資産として分類されるべきです。
CMMC 2.0における対象外資産の定義
CMMCスコープガイドによると、以下の資産が対象となります。
#FCI/CUIを保存、処理、または送信しないでください
#対象資産のセキュリティに直接影響を与えない
#FCI/CUI環境から完全に隔離されている
これらは対象外資産として分類されます。
商業サービス部門は公開されている情報のみを処理し、FCIとのやり取りがないため、その資産はCMMCレベル1評価の対象外となります。
他の回答が間違っている理由
A) FCI資産
#誤り。FCI資産とは、FCIを保存、処理、または送信する資産のみを指します。商業サービス部門はFCIを取り扱っていないため、その資産は対象外です。
B) 特殊資産
#誤り。特殊資産とは、モノのインターネット（IoT）、運用技術（OT）、および試験装置を指します。これらは、一般的な商業サービス部門には適用されません。
D) 運用技術資産
#誤り。運用技術（OT）資産には、産業制御システム、SCADA、製造設備などが含まれますが、これらはこのシナリオとは関係ありません。
CMMC公式資料
CMMC 2.0 スコープガイド - レベル1およびレベル2
CMMC評価プロセス（CAP）文書
したがって、公式のCMMCスコープ設定ガイダンスに基づくと、オプションC（対象外資産）が正解です。

最新問題: **103**
評価チームは、OSCの要請に基づき、レベル2の評価を実施しています。チームは、提供された証拠に基づいて診療行為の採点を開始しました。診療行為がMET（基準を満たしている）と評価されるかどうかを判断するために、評価チームに最低限求められることは何ですか？
A. すべての対照群について、3種類の証拠すべてが文書化されています。
B. ３種類の証拠のうち 1つを検討し、採用する。
C. 以下のいずれかを完了してください。2 つのアーティファクトを検査し、1 つの制御の満足のいくデモンストレーションを観察するか、OSC 担当者から 1 つの確認を受けます。
D. 以下のうち2つを完了する :1つのアーティファクトを検査する、1つの制御の満足のいくデモンストレーションを観察する、またはOSC職員から1つの確認を受ける。
Answer: D (メーッセージを残す**)**
この質問は、CMMC評価チームがレベル2評価において、ある診療所をMETと評価するために必要な最低限の証拠要件に関するものです。
The CMMC Level 2 assessment must align withNIST SP 800-171and follow the procedures outlined in theCMMC Assessment Process (CAP) Guide v1.0, particularly aroundevidence collection and scoring methodology.
#Step 1: Refer to the CMMC Assessment Process (CAP) Guide v1.0
CAP v1.0 - Section 3.5.4: Evaluate Evidence and Score Practices
"To assign a MET determination, the Assessment Team must collect and corroborate at least two types of objective evidence: either through examination of artifacts, interviews (affirmation), or testing (demonstration)." This meansat least two typesof the following evidence are required:
Examine(documentation/artifacts),
Interview(affirmation from personnel),
Test(demonstration of implementation).
#Step 2: Clarify the Official Minimum Standard for a Practice to be Scored MET The CAP explicitly states:
"A practice can only be scored MET when a minimum oftwo types of evidencefrom the E-I-T (Examine, Interview, Test) triad are successfully collected and evaluated." Theevidence types must come from two different categories, for example:
An artifact(Examine)+ an interview affirmation(Interview),
A demonstration(Test)+ an interview(Interview),
Etc.
This cross-validation ensures that the control isimplemented, documented, and understoodby personnel - a core principle in assessing effective cybersecurity implementation.
#Why the Other Options Are Incorrect
A). All three types of evidence are documented for every control

#Incorrect:While collecting all three types (E-I-T) strengthens the assessment, theminimum requirementis onlytwo. Collecting all three isnot requiredfor a practice to be scoredMET.
B). Examine and accept evidence from one of the three evidence types
#Incorrect:This fails to meet theminimum two-evidence-type requirementset by the CAP. Single-source evidence is not sufficient to score a practice as MET.
C). Complete one of the following; examine two artifacts, observe one demonstration, or receive one affirmation
#Incorrect:Even if two artifacts are examined,this is still only one type of evidence(Examine). The CAP requires twotypes- not two instances of the same type.
#Why D is Correct
D). Complete two of the following: examine one artifact, either observe a satisfactory demonstration of one control or receive one affirmation from the OSC personnel.
#This directly reflects theCAP's requirement for collecting two different types of objective evidenceto determine a practice is MET.
BLUF (Bottom Line Up Front):
To score a CMMC Level 2 practice asMET, the Assessment Team must collecta minimum of two distinct types of evidence- from theExamine, Interview, Test (E-I-T)categories. This requirement is clearly stated in the CMMC Assessment Process (CAP) v1.0.

最新問題**: 104**
各実践および／またはプロセスに必要な証拠は、以下の点を考慮して評価される。
A. 適切性と十分性
B. 適切性と徹底性
C. 十分性と徹底性
D. 十分性と適切性
Answer: (解答を表示する**)**
The CAP makes clear that evidence collected during the assessment is evaluated for both adequacy (does the evidence align with the requirement) and sufficiency (is there enough evidence to make a confident determination).
Supporting Extracts from Official Content:
* CAP v2.0, Evidence Collection Guidance: "Evidence must be evaluated for adequacy... and for sufficiency, to ensure enough information is available to support the assessor's determination." Why Option A is Correct:
* Evidence is assessed based on two qualities only: adequacy and sufficiency.
* "Thoroughness" and "appropriateness" are not official CAP terms for evidence evaluation.
References (Official CMMC v2.0 Content):
* CMMC Assessment Process (CAP) v2.0, Evidence Evaluation section.

最新問題**: 105**

OSCのレベル2評価において、満たされていない項目が15項目あります。これらの項目はすべてOSCに適用可能です。どのような判断を下すべきでしょうか？
A. OSCは、基準を満たしていない慣行を是正するために90日間の猶予が与えられる場合があります。
B. OSCは、満たされていない慣行を是正するためのオプションの対象ではありません。
C. OSCは、満たされていない慣行を是正するための選択肢の対象となる可能性があります。
D. OSCは、評価がキャンセルされた後に是正措置を受ける選択肢の対象ではありません。
Answer: (解答を表示する**)**
サイバーセキュリティ成熟度モデル認証（CMMC）2.0のコンテキストでは、レベル2の準拠を達成するには、認証を求める組織（OSC）がNIST SP 800-171リビジョン2に概説されている110のセキュリティ対策すべてを実装する必要があります。CMMCフレームワークでは、特定の欠陥に対処するために行動計画とマイルストーン（POA&M）を限定的に使用することが認められていますが、これは特定の基準を満たすことが条件となります。
CMMC最終規則によると、条件付きレベル2のステータスを取得するには、OSCは評価時に110点満点中88点以上の最低スコアを獲得する必要があります。この採点システムでは、110項目のセキュリティ要件それぞれに加重値が割り当てられ、一部の管理策は重要、その他は重要でないとみなされます。POA&Mメカニズムでは、最低スコアのしきい値を満たしていれば、OSCは重要でない不備に一時的に対処することができます。ただし、重要な管理策は評価時に完全に実装されている必要があり、延期してPOA&Mに含めることはできません。
あなた
15項目の基準を満たしていない場合、OSCのスコアは必要な88ポイントの基準値を下回り、組織は条件付きレベル2の認定を受ける資格を失います。その結果、OSCはPOA&M（改善計画）を通じてこれらの不備を是正する選択肢を持ちません。代わりに、組織は必要なコンプライアンスレベルを達成するために、次の評価を受ける前に、基準を満たしていないすべての項目を完全に実施し、是正する必要があります。
この方針は、機密指定されていない管理情報（CUI）を取り扱う組織が、すべての重要および非重要セキュリティ要件に適切に対処していることを保証し、それによって防衛産業基盤内の機密情報の完全性とセキュリティを維持することを目的としています。
評価基準およびPOA&Mの使用に関する詳細なガイダンスについては、CMMC評価ガイドを参照してください。
- レベル2、および国防総省が提供する公式のCMMC文書。

最新問題**: 106**
After completing a Level 2 Assessment, a C3PAO is preparing to upload the Assessment Results Package to Enterprise Mission Assurance Support Service. Which document MUST be included as part of the final assessment results package?
A. 概要レベルの調査結果

B. 認証評価
C. All Daily Checkpoint logs
D. 最終報告書
Answer: D (メーッセージを残す**)**

有効な **CMMC-CCP** 問題集は GoShiken.com が提供された合格しやすい CMMC-CCP 試験問題集！ GoShiken.com が最新の **CMMC-CCP** 試験問題集を提供しています。GoShiken.com CMMC-CCP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CMMC-CCP 問題集をゲットする人はこちら: https://www.goshiken.com/Cyber-AB/CMMC-CCP-mondaishu.html (**23030%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題**: 107**
営業部長は会議で、送信したメールの一部について、メールのマーク付けが正しく行われていないというフィードバックを営業チームから受け取ったと述べました。営業部長は、メールのマーク付け方法に関する情報について、営業チームにどの研修を勧めるべきでしょうか？
A. C3PAO CUI マーキング入門
B. NARA CUI マーキング入門
C. CMMC-AB CUI 採点入門
D. FBI CUIマーキング入門
Answer: B (メーッセージを残す**)**

最新問題**: 108**
実際の状況と期待される行動を比較する評価方法はどれですか？
A. コンパイル
B. インタビュー
C. テスト
D. 検査する
Answer: (解答を表示する**)**

最新問題**: 109**
What type of criteria is used to answer the question "Does the Assessment Team have the right evidence?"
A. Adequacy criteria
B. Objectivity criteria
C. Sufficiency criteria
D. Subjectivity criteria

Answer: (解答を表示する**)**
In the context of CMMC 2.0 assessments, thesufficiency criteriaare used to determine whether the assessment team has gathered enough evidence to support their conclusions about compliance with a given requirement.
* Definition of Sufficiency Criteria:
* Sufficiency refers to thequantityandcompletenessof the evidence collected during an assessment.
* This ensures that the evidence collected isenough to support an objective and valid determinationof compliance.
* Why Sufficiency Matters in CMMC 2.0:
* Assessors must ensure that the amount of evidence collected isadequate to substantiate findingswithout doubt or gaps.
* This prevents situations where an organization might claim compliance but lacks thenecessary documentation, technical evidence, or procedural validationto prove it.
* Official CMMC 2.0 References:
* TheCMMC Assessment Process (CAP) Guidedefines sufficiency as a key factor in validating assessment findings.
* According toCMMC 2.0 Level 2 Scoping Guidance, assessors must apply sufficiency criteria when reviewingartifacts, documentation, interviews, and system configurations.
* TheDoD CMMC Assessment Guide(aligned with NIST SP 800-171A) emphasizes that compliance decisions must besupported by a sufficient amount of verifiable evidence.
* Comparison with Other Criteria:
* Adequacy Criteria# Focuses onqualityof the evidence, not the quantity.
* Objectivity Criteria# Ensures evidence isunbiased and impartial, not necessarily complete.
* Subjectivity Criteria# Not applicable in CMMC since assessments must beobjective and based on factual evidence.
Step-by-Step Breakdown:Conclusion:To verify compliance in CMMC 2.0 assessments, the assessment team must ensuresufficientevidence is available to support a determination. This makes"Sufficiency Criteria" (Option C)the correct answer.

最新問題**: 110**
実際の状況と期待される行動を比較する評価方法はどれですか？
A. テスト
B. 検査する
C. コンパイル
D. インタビュー
Answer: A (メーッセージを残す**)**
CMMC評価方法の理解サイバーセキュリティ成熟度モデル認証（CMMC）2.0は、NIST SP 800-171A評価方法論に準拠しており、これには3つの主要な評価方法が含まれます。
* 調査 - ポリシー、手順、システム構成、およびドキュメントを確認します。

* インタビュー - 担当者と面談し、セキュリティ対策に関する理解度と実行状況を確認する。
* テスト - セキュリティ制御が期待どおりに機能するかどうかを判断するために、実際の技術的または運用上のテストを実施する。
* 「テスト」とは、実際に指定された条件と期待される動作を比較する方法です。
* これは、システムが要求どおりに動作するかどうかを確認するために、手順、構成、または自動化ツールを実行することを含みます。
例えば、ポリシーで多要素認証（MFA）を強制する必要があると規定されている場合、テストではMFAなしでログインを試みて、期待どおりにアクセスがブロックされるかどうかを確認します。
* NIST SP 800-171A ガイド（CUIの評価手順）では、テストを次のような評価方法として定義しています。
* セキュリティ制御が機能していることを積極的に検証する
* 現実世界の攻撃シナリオをシミュレートします
* 文書ではなくシステムアクションを通じてコンプライアンスをチェックする
* B. 検査する（不正解）
* 調査とは、ポリシー、手順、または構成を確認することのみを指し、システムの動作を積極的にテストするものではありません。
* C. コンパイル（誤り）
* 「コンパイル」は、CMMC 2.0 または NIST SP 800-171A の評価方法ではありません。
* D. インタビュー（不正解）
インタビューは従業員から意見を収集するために用いられるが、実際の状況と期待される行動を比較するものではない。
正解はAです。テストは、想定されるセキュリティ条件に対してシステムのパフォーマンスを積極的に検証するためです。
参考文献：
NIST SP 800-171A、「CUIのセキュリティ要件の評価」
CMMC 2.0評価プロセス（CAP）ガイド
国防総省CMMCスコープ設定および評価ガイドライン

最新問題: **111**
評価プロセスの計画段階で、C3PAOのスタッフは、CMMCレベル2評価を要求したOSCに関連するさまざまな組織をレビューしています。評価に参加するものの、エンタープライズ評価が実施されない限りCMMCレベルを取得できない、本部組織の外部の人、プロセス、およびテクノロジーを表す用語はどれですか？
A. ホストユニット
B. 支援組織／部署
C. 組織
D. 調整ユニット

Answer: B (メーッセージを残す)

最新問題: **112**
監査 説明責任 AU）分野には、以下の実践が含まれます。
A. レベル1。
B. レベル2。
C. レベル1とレベル2。
D. レベル1とレベル3。
Answer: B (メーッセージを残す)
監査および説明責任 (AU) ドメインは、NIST SP 800- の 14 のセキュリティ要件ファミリーの 1 つです。
171 Rev. 2 は、CMMC 2.0 レベル 2 で完全に採用されています。
* A. レベル1#不正解
* CMMCレベル1には、FAR 52.204-21の基本的な17の安全対策要件のみが含まれており、監査および説明責任 AU）の実践は含まれていません。
* B. レベル2#正解
* AUドメインはレベル2で必須であり、これはNIST SP 800-171に準拠しています。
* CMMC 2.0 レベル 2 には 110 のセキュリティ管理項目が含まれており、その中で AU 関連の管理項目はログ記録、監視、および説明責任に重点を置いています。
* C. レベル1と2#不正解
レベル1では、監査および説明責任に関する慣行は義務付けられていません。
* D. レベル1と3#不正解
* CMMC 2.0にはレベル1、2、3しかなく、AUはレベル2に含まれているため、レベル3はこの回答には関係ありません。
* NIST SP 800-171 Rev. 2（監査および説明責任 - ファミリー3.3）
* AUドメインは、監査ログの生成、保持、および説明責任に焦点を当てたセキュリティ制御3.3.1～3.3.8で構成されています。
* CMMC 2.0 レベル2の実践（NIST SP 800-171に準拠）
* AU（監査および説明責任）の実践はレベル2でのみ必須です。
提示された選択肢の分析：正解を裏付ける公式資料：結論AUドメインはCMMC 2.0レベル2にのみ適用されるため、正解は次のようになります。
#B. レベル2。

最新問題: **113**
CCP（認定コンサルティングプロバイダー）がOSC（オープンサービス企業）にコンサルティングサービスを提供しています。CCPはOSCのCMMCレベル2評価の準備を進めています。OSCはCCPに対し、CMMC評価範囲の決定責任者と、その評価範囲の妥当性を確認する責任者は誰かを尋ねました。CCPはどのように回答すべきでしょうか？
A. 「OSCがCMMC評価範囲を決定し、CCPがCMMC評価範囲を検証します。」

B. OSCがCMMC評価範囲を決定し、C3PAOがCMMC評価範囲を検証する。」
C. CMMC主任評価者がCMMC評価範囲を決定し、OSCがCMMC評価範囲を検証する。」
D. CMMC C3PAOがCMMC評価範囲を決定し、主任評価者がCMMC評価範囲を検証する。」

Answer: B (メーッセージを残す)

ステップ1 :CMMC評価範囲の決定を理解する
In a CMMC Level 2 assessment, the Organization Seeking Certification (OSC) is responsible for identifying the assessment scope based on the CMMC Scoping Guidance provided by the Cyber AB (Cyber Accreditation Body) and DoD.
The OSC must determine which assets and systems handle Controlled Unclassified Information (CUI) and categorize them accordingly.
Reference:
CMMC Scoping Guidance for Level 2, which outlines asset categorization and scoping considerations.
Step 2: Role of the C3PAO in Scope Validation
Once the OSC has determined its CMMC assessment scope, a CMMC Third-Party Assessment Organization (C3PAO) is responsible for validating the scope during the assessment planning phase.
The C3PAO reviews the OSC's scope to ensure it aligns with DoD's scoping guidance, ensuring that all relevant assets, networks, and policies required for CMMC Level 2 certification are correctly identified.
If there are discrepancies, the C3PAO works with the OSC to adjust the scope before proceeding with the assessment.
Reference:
CMMC Assessment Process (CAP) Guide, which describes the scope validation responsibilities of a C3PAO.
Step 3: Why Other Answer Choices Are Incorrect
Choice A (Incorrect): A CCP (Certified CMMC Professional) does not have the authority to validate the scope. Their role is to guide and consult, but final validation is the C3PAO's responsibility.
Choice C (Incorrect): The CMMC Lead Assessor (part of the C3PAO team) does not determine the scope; instead, the OSC does.
Choice D (Incorrect): The C3PAO validates the scope but does not determine it-this is the OSC's responsibility.
Final Confirmation of Correct Answer:
OSC determines the CMMC Assessment Scope.
C3PAO validates the CMMC Assessment Scope.
Thus, the correct answer is B. "The OSC determines the CMMC Assessment Scope, and the C3PAO validates the CMMC Assessment Scope."

最新問題: **114**
SI.L1-3.14.2 「組織の情報システム内の適切な場所で悪意のあるコードからの保護を提供する」を評価する際、OSCのすべてのワークステーションとサーバーに悪意のあるコードからの保護のためのウイルス対策ソフトウェアがインストールされていることが確認されました。ウイルス対策ソフトウェア管理のための集中管理コンソールが設置されており、すべてのデバイスに最新のウイルス対策パターンが適用されていることが記録から示されています。
主任評価者が証拠に関して下すべき最善の判断とは何でしょうか？
A. 十分であり、監査結果はMETと評価できます。
B. 不十分であり、監査結果は「未達成」と評価される。
C. 十分であり、主任評価者はさらなる証拠を求めるべきである。
D. 不十分であり、主任評価者はさらなる証拠を求めるべきである。
Answer: A (メーッセージを残す)
SI.L1-3.14.2 の理解: 悪意のあるコードからの保護の提供CMMC レベル 1 プラクティス SI.L1-
3.14.2は、NIST SP 800-171の要件3.14.2に基づいており、組織には以下のことが求められます。
- 悪意のあるコードに対する保護対策を実施する（例ウイルス対策ソフト、エンドポイントセキュリティソフトウェア）。
* すべての適切な場所（ワークステーション、サーバー、ネットワークエントリポイントなど）でカバレッジが確保されていることを確認してください。
* 保護メカニズムを最新の状態に保つ（例：定期的な署名の更新、ポリシーの適用）。
「MET」評価の評価基準：診療所がMETであるかどうかを判断するために、主任評価者は以下の点を確認する必要があります。
#すべてのワークステーションとサーバーにウイルス対策ソフトウェアまたはエンドポイント保護ソフトウェアがインストールされています。
#このソリューションは一元管理されており、一貫したポリシー適用を保証します。
#署名の更新は最新の状態であり、システムは新たな脅威から保護されています。
#ログまたはレポートは、アクティブな監視と更新を示しています。
正解が「A. 十分であり、監査結果はMETと評価できる」である理由は？提供された証拠は、SI.L1-3.14.2に必要なすべての要件を満たしていることを確認しています。
#すべてのワークステーションとサーバーにウイルス対策ソフトがインストールされています#インストール要件を満たしています。
#集中管理コンソールが導入されています#一貫した執行を保証します。
#記録によると、ウイルス対策シグネチャは最新です#システム保護が最新であることを確認します。
証拠が要件を満たしているため、この慣行はMET（要件を満たしている）と評価されるべきである。
* B. 不十分であり、監査結果は「未達成」と評価される。# 不正解

提出された証拠は必要な要件をすべて満たしているため、当該慣行は 要件を満たしていない」と評価されるべきではありません。
* C. それで十分であり、主任評価者はさらなる証拠を求めるべきである # 不正解
十分な証拠が既に存在する場合は、追加の証拠は不要です。
* D. 不十分であり、主任評価者はさらなる証拠を求めるべきである # 不正解
提出された証拠は管理要件を満たしており、十分である。
他の回答が間違っているのはなぜですか？
* CMMC評価プロセス（CAP）文書
* 十分な証拠が提示された場合、その実践はMETとしてマークできることを指定します。
* NIST SP 800-171（要件3.14.2）
* アクティブなアップデートを備えたウイルス対策ソフトが満たす、標準的な形式的コード保護を定義します。
* CMMC 2.0 レベル 1 (基礎) 要件
* ウイルス対策ソフトのインストールやアップデートなどの基本的なサイバーセキュリティ対策がSI.L1-3.14.2の準拠を満たしていることを明確にします。
この回答を裏付けるCMMC 2.0の参考文献：
最終回答 #A. 十分であり、監査結果はMETと評価できます。

最新問題**: 115**
OSCのレベル2評価において、満たされていない項目が15項目あります。これらの項目はすべてOSCに適用可能です。どのような判断を下すべきでしょうか？
A. OSCは、基準を満たしていない慣行を是正するために90日間の猶予が与えられる場合があります。
B. OSCは、満たされていない慣行を是正するためのオプションの対象ではありません。
C. OSCは、満たされていない慣行を是正するための選択肢の対象となる可能性があります。
D. OSCは、評価がキャンセルされた後に是正措置を受ける選択肢の対象ではありません。
Answer: C (メーッセージを残す**)**
CMMCモデルおよび評価ガイド、特に行動計画とマイルストーン（POA&M）および是正期間に関する規則によれば、認証を求める組織（OSC）は、評価に完全に不合格となることなく、 未達成」の特定の慣行を是正して 達成」ステータスを達成するための限定的な機会が与えられます。
CMMCエコシステムプロトコルに基づいた内訳は以下のとおりです。
180日間のPOAとMルール：CMMCレベル2では、優先度の高い項目（通常 採点方法論で5ポイントの値）でない限り、特定の業務にPOAとMを使用することが許可されています。OSCが
 未達成」と判断された慣行については、改善命令（POA & M）の対象となる場合、是正のために最大180日間の猶予が与えられます。

是正期間（評価完了）：評価プロセス自体には、「是正期間」（特定のC3PAO方法論とCMMC評価プロセスに応じて1〜90日間の期間と呼ばれることが多い）があり、OSCは最終報告書が提出される前に評価者によって特定された軽微な問題を修正することができます。
適格基準: 質問では、「未達成」のプラクティスが 15 項目あるとされています。これは多い数ですが、CMMC ルールでは、プラクティスの数だけに基づいて OSC を自動的に不適格とするのではなく、プラクティスの種類 (重み) と結果として得られるスコアに基づいて判断します。条件付き「達成」(POA および M 経由) の資格を得るには、OSC は最低スコア (多くの場合、合計ポイントの 80%) を達成する必要があり、「未達成」のプラクティスは CMMC ルールで必須の「達成」(POA および M が認められない) として指定されているものであってはなりません。
「C」が正解である理由：15項目の「未達成」項目の具体的な重みや合計スコアが不明なため、それらが是正される（A）か、対象外である（B）かを断定することはできません。しかし、CMMC評価フレームワークの下では、OSCがスコアの閾値を満たし、かつ具体的な項目がそれを許容する場合、是正フェーズに進むか、またはPOA & Mを利用してギャップを埋めることができる可能性があります。
参考資料：
CMMC評価プロセス（CAP）：評価の各段階（「是正期間」を含む）を定義します。
32 CFR Part 170 (CMMCプログラム規則): POA & Msの具体的な要件、180日間の期限、および条件付き認証の資格を得るために必要なスコアリングパラメータの概要を示します。

最新問題: **116**
サイバーセキュリティ規制を遵守しないことで政府を故意に欺いた企業は、以下の責任を問われるリスクがあります。
A. 契約金額にサイバー賠償法に定められた違約金を加えた金額
B. 契約金額に虚偽請求法に定められた罰金を加えた金額
C. 契約金額の3倍に加え、サイバー賠償法に定められた違約金
D. 契約金額の3倍に加え、虚偽請求法に定められた罰金
Answer: D (メーッセージを残す)
虚偽請求法（米国法典第31編第3729条〜第3733条）は、連邦政府との契約を受注または維持するために、法令遵守状況を故意に偽って申告した企業に責任を課すものです。罰則には、政府の損失額の3倍の賠償金に加え、請求ごとに追加の罰金が科せられます。
公式コンテンツからの補足抜粋：
* 虚偽請求法：「故意に政府に虚偽の請求を行った者は、政府の損害額の3倍に加えて罰金を科される。」
* 司法省サイバー詐欺対策イニシアチブ（2021年）：FCAはサイバーセキュリティ要件への準拠を偽った事例にも適用されることを確認した。
選択肢Dが正解である理由：
適用される法律は虚偽請求法であり、「サイバー請求法」（そのような法律は存在しない）ではありません。

* FCAは損害賠償額の3倍に加えて罰金を規定しており、これはオプションDと完全に一致する。
参考文献（CMMC v2.0 公式ガバナンスおよびソース文書）：
* 虚偽請求法（米国法典第31編第3729条～第3733条）。
* 司法省のサイバー詐欺対策イニシアチブ（2021年）は、CMMC関連のコンプライアンスに関する虚偽表示に適用された。

最新問題: **117**
職業倫理規定において、プロフェッショナリズムの実践には何が求められていますか？
A. 評価結果について断言しないでください。
B. 許可なく資料を複製しないでください。
C. CMMCに関するすべての取引において不正行為を控えること。
D. 発見または受信したすべての情報のセキュリティを確保する。
Answer: C (メーッセージを残す**)**

最新問題: **118**
主任評価者および評価チームのメンバーは、必要に応じて、評価最終勧告結果概要から何日以内に、(OSCの更新されたPOA&Mと付随する証拠または予定されている収集物の正確性と妥当性をレビューする必要がありますか?
A. 90日間
B. 180日
C. 270日
D. 360日
Answer: B (メーッセージを残す**)**
CMMC 2.0 の評価プロセスでは、評価最終推奨事項概要の後、主任評価者と評価チームのメンバーは、認証を求める組織 (OSC) の更新された行動計画とマイルストーン (POA&M) および付随する証拠または予定されている収集物の正確性と妥当性を 180 日以内に確認する必要があります。
* CMMC評価プロセス（CAP）では、組織は最初の評価後、特定された欠陥に対処するために最大180日間の猶予が与えられると規定されています。
* この期間中、OSCは遵守を証明するための追加証拠を添えてPOA&Mを更新することができます。
関連するCMMC 2.0の参照資料：
* A. 90日 # 不正解
* CMMC CAPでは、POA&Mの更新に90日間の制限は設けられていません。代わりに、180日間が標準的な期間となっています。
* B. 180日 # 正解
* CMMC評価プロセスのガイドラインに従い、主任評価者とチームは180日以内に更新内容を確認する必要があります。
* C. 270日 #.偽

* CMMCの公式文書には、270日間のレビュー期間に関する記述はありません。
* D. 360日 # 不正解
コンプライアンスを維持するためには、このプロセスは360日よりもはるかに早く完了する必要があります。
正解が180日（B）である理由は？
* CMMC評価プロセス（CAP）文書
* OSCがPOA&Mを更新し、審査のための証拠を提出するための180日間の期間を定義します。
* CMMC 2.0 公式ガイドライン
* 組織は再評価の前に、不備を是正するために最大180日間の猶予が与えられることを規定している。
この回答を裏付けるCMMC 2.0の参考文献：

最新問題: **119**
Which assessment method describes the process of reviewing, inspecting, observing, studying, or analyzing assessment objects (i.e., specification, mechanisms, activities)?
A. Test
B. Assess
C. Examine
D. Interview
Answer: C (メーッセージを残す)
Understanding the "Examine" Assessment Method in CMMC 2.0CMMC 2.0 usesthree assessment methodsto evaluate security compliance:
* Examine- Reviewing, inspecting, observing, studying, or analyzing assessment objects (e.g., policies, system documentation).
* Interview- Speaking with personnel to verify knowledge and responsibilities.
* テスト - システム構成を確認するための技術的な検証を実行します。
* CMMC評価プロセス（CAP）では、評価対象（ポリシー、手順、構成、ログなど）をレビューまたは分析するために使用される方法として、検査を定義しています。
関連するCMMC 2.0の参照資料：
* A. テスト番号 不正解
* 「テスト」とは、セキュリティを検証するために機能を実行することを指します（例ライブシステムテストを通じてアクセス制御を検証する）。
* B. 評価 # 不正解
* 「評価する」は広範な用語です。CMMCでは、文書をレビューする方法として「検査する」を明確に定義しています。
* C. 検査 # 正解
* 「調査」とは、ポリシー、手順、構成、またはログを確認するための正式な用語です。
* D. インタビュー # 不正解
* 「インタビュー」とは、文書分析ではなく、担当者との口頭での話し合いを指します。

正解が「調べる」(C)である理由は？
* CMMC評価プロセス（CAP）文書
*「調査する」とは、評価対象（ポリシー、手順、ログ、文書など）を分析することと定義します。
* NIST SP 800-171A
* セキュリティ制御と構成を確認する方法として「検査」を指定します。
この回答を裏付けるCMMC 2.0の参考文献：

最新問題: **120**
FCIまたはCUIを取り扱う組織に対し、必要なサイバーセキュリティ成熟度レベルを判断するための評価を義務付けているのは、どの機関ですか？
A. 国防総省
B. CISA
C. NIST
D. CMMC-AB
Answer: A (メーッセージを残す**)**
ステップ1：CMMCにおける国防総省の役割を理解する
米国国防総省（DoD）は、連邦契約情報（FCI）または管理対象非機密情報（CUI）を取り扱う組織に対し、CMMC 2.0に基づき必要なサイバーセキュリティ成熟度レベルを判断するための評価を受けることを義務付けている機関です。
この要件は、FCIまたはCUIを取り扱う請負業者にCMMC認証を義務付けるDFARS 252.204-7021条項に由来する。
参照：
国防総省CMMC 2.0プログラムの概要
DFARS 252.204-7021（CMMC要件）
ステップ2：国防総省のサイバーセキュリティ成熟度レベル
国防総省は、契約に関わる情報の機密性に基づいて、契約に必要なサイバーセキュリティ成熟度レベルを決定します。
CMMCレベル1 - FCI（基本的なサイバー衛生）を扱う組織に必須。
CMMCレベル2 - CUIを取り扱う組織に必須（NIST SP 800-171に準拠）。
CMMCレベル3 - 価値の高いCUIを取り扱い、高度な持続的脅威（APT）に直面している組織に必須（NIST SP 800-172のサブセットに準拠）。
参照：
CMMC 2.0 モデルドキュメント
セキュリティ管理に関するNIST SP 800-171および800-172
ステップ3：他の選択肢が間違っている理由
B) CISA（不正解）：
サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）は国家のサイバーセキュリティを担当しているが、CMMC評価を義務付けてはいない。
C). NIST（誤り）：

米国国立標準技術研究所（NIST）はセキュリティフレームワーク（例NIST SP）を提供しています。
800-171) だが、CMMC 準拠を強制するものではない。
D). CMMC-AB（不正解）：
Cyber AB（旧CMMC-AB）は、C3PAOの認定とCMMCエコシステムの監督を担当していますが、どの組織が評価を必要とするかを決定する権限はありません。
正解の最終確認：
国防総省は、FCI（外国感染物またはCUI（機密情報を取り扱う組織に対し、CMMC（コンピュータ化保守認証）への準拠を義務付けている。
CMMCの要件は、国防総省の契約におけるDFARS条項を通じて強制される。
したがって、正解はA.国防総省です。

最新問題**: 121**
NIST SP 800-88 改訂版1「メディアサニテーションに関するガイドライン」に記載されているデータ廃棄のカテゴリを要約する言葉はどれですか？
A. 浄化、浄化、破壊
B. 編集済みコンテンツを削除し、破棄する
C. クリア、上書き、パージ
D. 消去、上書き、破壊
Answer: (解答を表示する**)**
NIST SP 800-88 Rev. 1とメディアサニタイゼーションの理解
NIST特別刊行物（SP）800-88改訂版1「メディアサニタイズに関するガイドライン」は、不正アクセスやデータ復旧を防止するために、さまざまな種類のストレージメディアからデータを安全に廃棄するためのガイダンスを提供します。
NIST SP 800-88 Rev. 1におけるデータ廃棄の3つのカテゴリ
クリア
論理的な手法を用いてメディアからデータを削除するため、標準的なシステム機能では復元が困難になる。
例：ハードドライブ上のすべてのデータをバイナリのゼロまたはイチで上書きする。
適用対象: 磁気メディア、ソリッドステートドライブ (SSD)、および不揮発性メモリ。メディアが同じセキュリティ環境内で再利用される場合。
パージ
高度な技術を用いて、フォレンジックツールを使ってもデータ復旧を不可能にする。
例：磁気ハードドライブの消磁、または暗号化消去（暗号化キーの削除）。
適用対象: 組織の管理下から離れるメディア、または「クリア」よりも高いレベルの保証を必要とするメディア。
破壊する
物理的にメディアを損傷させ、データ復旧を不可能にする。
例：ストレージデバイスの細断、焼却、粉砕、または分解。

適用対象：永久に消去する必要のある、極めて機密性の高いデータ。
A. クリア、パージ、デストロイ」が正しい理由は？
B) クリア、編集、破棄（誤り）- 「編集」は文書の消去に使用される用語であり、データの破棄に使用される用語ではありません。
C). クリア、上書き、パージ（誤り）- 「上書き」は「クリア」内のメソッドですが、NIST SP 800-88 ではトップレベルのカテゴリではありません。
D) クリア、上書き、破棄 (不正解) - 「上書き」は「クリア」のサブメソッドですが、「パージ」が欠落しているため、これは不正解です。
結論
正解はAです。クリア、パージ、破棄。これらはNIST SP 800-88リビジョン1におけるデータ廃棄の公式な3つのカテゴリです。
参考文献：
NIST SP 800-88 Rev. 1 - 培地サニタイゼーションに関するガイドライン
CMMC 2.0 メディア廃棄に関するセキュリティ対策（NISTガイダンスに準拠）

有効な **CMMC-CCP** 問題集は GoShiken.com が提供された合格しやすい CMMC-CCP 試験問題集！ GoShiken.com が最新の **CMMC-CCP** 試験問題集を提供しています。GoShiken.com CMMC-CCP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CMMC-CCP 問題集をゲットする人はこちら: https://www.goshiken.com/Cyber-AB/CMMC-CCP-mondaishu.html (**23030%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **122**
下請業者が有効なCMMC認証を取得していることを確認する責任は誰にありますか？
A. CMMC-AB
B. OUSD A&S
C. 国防総省機関またはクライアント
D. 請負業者組織
Answer: D (メーッセージを残す**)**
DFARSおよびCMMCの要件に基づき、主契約者は下請け業者が必要なCMMCレベルを満たしていることを確認する責任を負います。国防総省、サイバー空軍、国防次官補（調達調達担当）のいずれも、下請け業者の認証を直接管理していません。
公式コンテンツからの補足抜粋：
* DFARS 252.204-7021: 「請負業者は、下請け業者が取り扱う情報に対して適切なCMMCレベルの認証を取得していることを確認しなければならない。」オプションDが正しい理由:
コンプライアンス責任は、請負業者のサプライチェーン全体にわたって及ぶ。

* CMMC-AB（サイバーAB）は評価者を認定するが、下請け業者を監視するわけではない。
* OUSD A&Sは契約レベルでの方針策定は行うが、執行は行わない。
* 国防総省機関は、契約／授与の監督レベルでのみ法令遵守を要求している。
参考文献（CMMC v2.0公式コンテンツ）：
*DFARS 252.204-7021。
* CMMCモデルv2.0のガバナンスガイダンス。

最新問題: **123**
企業のCMMCレベル1自己評価の範囲を決定する際、契約管理者は自社のITインフラストラクチャを管理するホスティングプロバイダーを含めます。サードパーティ組織を最も適切に表す資産タイプはどれですか？
A. テクノロジー
B. ESPs
C. 設備
D. 人々
Answer: B (メーッセージを残す**)**

最新問題: **124**
企業のCMMCレベル1自己評価の範囲を決定する際、契約管理者は自社のITインフラストラクチャを管理するホスティングプロバイダーを含めます。サードパーティ組織を最も適切に表す資産タイプはどれですか？
A. ESP
B. 人々
C. 設備
D. テクノロジー
Answer: (解答を表示する**)**
企業が自社のインフラストラクチャの管理に第三者のITプロバイダーを利用する場合、これらの組織はCMMCのスコープガイドラインにおいて外部サービスプロバイダー（ESP）として分類されます。
ステップごとの解説 #1. ESPとは何ですか？
外部サービスプロバイダー（ESP）とは、以下のような第三者組織のことです。
ITサービス、クラウドホスティング、およびマネージドセキュリティソリューションを提供します。
請負業者に代わって、FCIまたはCUIを処理、保管、または送信する。
FCIまたはCUIを取り扱う場合は、OSCと同じセキュリティ要件を満たす必要があります。
企業がITインフラストラクチャの管理をホスティングプロバイダーに依存している場合、そのプロバイダーはCMMCのスコープガイドラインにおけるESP（エンタープライズサービスプロバイダー）に該当します。
#2. 他の選択肢が間違っている理由：
（B）人々#

誤り：ESPは組織であり、個人ではありません。
（C）施設
誤り：施設とは、オフィスビルやデータセンターなどの物理的な場所を指し、第三者サービスプロバイダーを指すものではありません。
（D）テクノロジー
誤り：ESPはテクノロジーサービスを提供しますが、CMMCにおけるサードパーティITプロバイダーの正しい用語は「テクノロジー」ではなくESPです。CMMCレベル1スコープガイドでは、外部サービスプロバイダー（ESP）をITインフラストラクチャとセキュリティサービスを管理するサードパーティ組織と定義しています。
CMMCドキュメントからの最終検証：したがって、正解は次のとおりです。
A. ESP（外部サービスプロバイダー）

最新問題: **125**
On a Level 2 Assessment Team, what are the roles of the CCP and the CCA?
A. The CCP leads the Level 2 Assessment Team, which consists of one or more CCAs.
B. The CCA leads the Level 2 Assessment Team, which can include 3 CCP with US Citizenship.
C. The CCA leads the Level 2 Assessment Team, which can include a CCP regardless of citizenship.
D. The CCP leads the Level 2 Assessment Team, which can include a CCA. regardless of citizenship.
Answer: C (メーッセージを残す)
Step 1: Define Roles - CCP and CCA
CCP (Certified CMMC Professional):
Entry-level certification in the CMMC ecosystem.
Supports assessment activities under the supervision of a CCA.
May assist in consulting roles outside of formal assessments.
CCA (Certified CMMC Assessor):
Certified tolead assessmentsunder the CMMC model.
Requiredfor conductingLevel 2 formal assessments.
Can be part of a C3PAO assessment team or lead it.
Source: CMMC Assessment Process (CAP) v1.0, Section 2.3 - Assessment Team Composition
"Level 2 assessments must be led by a Certified CMMC Assessor (CCA), who may be supported by one or more CCPs."
Step 2: Citizenship Requirements
CAP v1.0 - Appendix B: Team Composition and Clearance Requirements
"All team members performing Level 2 assessments must be U.S. citizens when handling CUI, regardless of role." But forsupporting team members who do not handle CUIor inFCI-only scoping, there is no automatic exclusion based on citizenship.

So:
TheCCA leadsthe team.
CCPs can be team membersregardless of citizenship,unless restricted by contract or CUI handling needs.
#Why the Other Options Are Incorrect
A). The CCP leads the Level 2 Assessment Team...
#Incorrect. CCPscannot leadLevel 2 assessments.
B). The CCA leads... includes 3 CCP with US Citizenship.
#Incorrect. Citizenship is requiredonly when handling CUI, not a universal requirement.
D). The CCP leads...
#Again, CCPs donot have the authority to leadformal CMMC assessments.
レベル2評価チームを率いることができるのは、認定CMMC評価者（CCA）のみであり、契約上またはデータ機密性の範囲に基づいて市民権が要件とならない場合は、米国市民以外のCCP（認定認定専門家）もチームに含めることができます。

最新問題: **126**
2人のネットワーク管理者が協力して、CMMCへの準拠に向けたネットワーク構成を決定しようとしています。しかし、いくつかの細かい点で意見が食い違うことが分かりました。CMMCへの準拠を確実にするための最適な解決策はどれでしょうか？
A. CMMC評価ガイドおよびNIST SP 800-171を参照してください。
B. 最も規制の緩いネットワーク管理者の意見に従う。
C. 最も厳格な制御を行うネットワーク管理者の考えに従う。
D. 会社のCEOに相談してください。
Answer: A (メーッセージを残す**)**

最新問題: **127**
CMMCアセスメントの実施中に、OSCの担当者がアセスメント担当者にレビュー用の文書を提供します。この文書には、インシデント対応能力が確立されていること、およびインシデントの準備、検出、分析、封じ込め、復旧、ユーザー対応活動に関する情報が記載されています。この文書は、どのCMMCプラクティスを証明しているのでしょうか？
A. IR.L2-3.6.4: 事故による流出
B. IR.L2-3.6.3: インシデント対応テスト
C. IR.L2-3.6.1: インシデント対応
D. IR.L2-3.6.2: インシデント報告
Answer: C (メーッセージを残す**)**

最新問題: **128**
CMMCのスコープは、CUIが存在する場所に焦点を当てたシステム、アプリケーション、サービスを含むCUI環境を対象としています。
A. 受信および転送。

B. 保存、処理、送信。
C. 入力、編集、操作、印刷、閲覧。
D. 電子媒体、システムコンポーネントのメモリ、および紙媒体に存在する。
Answer: B (メーッセージを残す**)**
CMMCレベル2のスコープガイドでは、CUI資産には、管理対象非機密情報（CUI）を保存、処理、または送信するシステム、アプリケーション、およびサービスが含まれると概説しています。これらは、認証取得を目指す組織（OSC）におけるCUIの取り扱いを定義する3つの主要機能です。
手順ごとの詳細：
#1. CMMCで定義されているCUI資産
保存場所：CUIはハードドライブ、クラウドストレージ、またはデータベースに保存されます。
処理済み：CUIは、アプリケーションやユーザーによって積極的に使用、変更、または分析されています。
送信：CUIは、電子メール、ファイル転送、またはネットワーク通信を介してシステム間で送信されます。
#2. 他の選択肢が間違っている理由：
（A）受領および転送#
CUIの受領と移転はCUIの取り扱いの一部ではあるが、CUI資産に関するすべての責任を完全に網羅するものではない。
（C）入力、編集、操作、印刷、閲覧#
これらは処理内の特定のアクションですが、CMMCのスコープ設定に必要なストレージや送信は含まれません。
（D）電子媒体、システムコンポーネントメモリ、紙媒体に存在する# CUIは電子形式と物理形式で存在できますが、CMMCのスコープは、CUIが物理的に存在する場所ではなく、CUIがどのようにアクティブに管理されるか（保存、処理、送信）に焦点を当てています。
CMMCドキュメントに基づく最終検証：
CMMCレベル2スコープガイドでは、CUI資産はCUIの保存、処理、または送信における役割に基づいて分類されることが確認されています。
NIST SP 800-171もまた、これら3つの機能をCUI保護の重要な構成要素として定義している。

最新問題**: 129**
職業倫理規定において、プロフェッショナリズムの実践には何が求められていますか？
A. 許可なく資料を複製しないでください。
B. 評価結果について断言しないでください。
C. CMMCに関するすべての取引において不正行為を控えること。
D. 発見または受信したすべての情報のセキュリティを確保する。
Answer: C (メーッセージを残す**)**

CMMCの職業倫理規定において、プロフェッショナリズムの実践には何が求められているのか？
CMMC専門職行動規範（CoPC）は、認定CMMC評価者（CCA）および認定CMMC専門家（CCP）に対する倫理的および専門的な基準を定めています。プロフェッショナリズムには、CMMC関連のあらゆる活動における誠実さと高潔さが求められます。
手順ごとの詳細：
#1. プロフェッショナリズムには倫理的な行動が求められる
CoPCは、プロフェッショナリズムには以下が含まれると述べています。
評価に関連するすべての活動において、誠実に行動する。
サイバーセキュリティ対策に関する、真実かつ客観的な評価を提供する。
評価やコンプライアンスに関する欺瞞的または誤解を招くような主張を避ける。
#2. 他の選択肢が間違っている理由：
（A）許可なく資料を複製してはならない。
これは知的財産権（IP）保護の範疇に属し、プロ意識の問題ではありません。
（B）評価結果について断言しないこと#
評価者は証拠に基づいて所見を提示しなければならない。この規則は、虚偽または誤解を招くような主張をしないことに関するものであり、主張を一切避けることを意味するものではない。
（D）発見または受領したすべての情報のセキュリティを確保する#
これは機密保持の範疇に属し、プロ意識の範疇には属さない。
CMMCドキュメントに基づく最終検証：
CMMC専門職行動規範（CoPC）は、プロフェッショナリズムを、CMMC関連のあらゆる活動において誠実さと高潔さを要求するものと定義しています。
したがって、正解は次のとおりです。
#C. CMMCに関するすべての取引において、不正行為を控えること。

最新問題: **130**
CUI（機密情報）の識別と表示を担当する政府機関はどの組織ですか？
A. NARA
B. NIST
C. CMMC-AB
D. 国土安全保障省
Answer: A (メーッセージを残す**)**
ステップ 1: CUI (管理された非機密情報) を定義する CUI とは、適用される法律、規制、および政府全体のポリシーに従って保護または配布の管理が必要な情報ですが、大統領令 13526 号または原子力エネルギー法の下では機密情報として分類されていません。
#ステップ 2: CUI に対する権限 - NARA の役割 NARA - 国立公文書館および記録管理局、特に情報セキュリティ監督局 (ISOO) は、CUI プログラムの実施を担当する政府全体の執行機関です。
ソース：

32 CFR パート2002 - 管理対象非機密情報（CUI）
大統領令13556号 - 機密解除された管理情報
CUI レジストリ - https://www.archives.gov/cui
NARA:
CUIレジストリを管理し、
問題マーキングと取り扱いに関するガイダンス、
CUIのカテゴリと、法律または規制に基づくそれらの権限を定義します。
連邦政府機関および請負業者に対し、CUI（機密情報）に関する方針について研修および情報提供を行う。
B). NIST# NIST（米国国立標準技術研究所）は技術標準（例SP 800-171）だが、CUIを定義したりマークしたりするものではない。CUIが特定された後に、CUIを保護するのに役立つ。
C). CMMC-AB（現在はCyber AB）# Cyber ABはCMMCエコシステムの認定機関であり、政府機関ではなく、CUIの分類やマーキングに関する権限はありません。
D) 国土安全保障省 (DHS)# DHS は CUI を内部で取り扱い保護することはできますが、CUI プログラムの執行機関ではありません。
#他の選択肢が間違っている理由
NARAは、大統領令13556号に基づき、CUIレジストリおよび関連ポリシーを通じてCUIを定義、分類、およびマークする責任を負う米国政府の公式機関です。

最新問題**: 131**
CMMC評価プロセスのどの段階で、証拠の特定、インベントリの取得、および検証を行う作業が含まれますか？
A. フェーズ1：評価の計画と準備
B. フェーズ2：評価の実施
C. フェーズ3：推奨評価結果の報告
D. フェーズ4：未解決の評価問題の是正
Answer: (解答を表示する**)**
CMMC評価プロセスを理解するCMMC評価プロセス（CAP）は4つのフェーズで構成され、各フェーズには特定のタスクと目的があります。
* フェーズ 1: 評価の計画と準備 - 評価の計画、スケジュール設定、および準備。
* フェーズ 2: 評価の実施 - 証拠の収集と検証、インタビューの実施、およびコンプライアンスの評価。
* フェーズ 3: 推奨評価結果の報告 - 調査結果を文書化し、結果を報告する。
* フェーズ 4: 未解決の評価問題の是正 - 組織が欠陥に対処できるようにする。
「フェーズ2：評価の実施」が正しい理由とは？フェーズ2：評価の実施では、評価チームは以下の主要な活動を実施します。
#コンプライアンス検証に必要な証拠を特定する。
#アーティファクト（セキュリティポリシー、構成、ログなど）の取得とレビュー。

#CMMCの実施要件に対する証拠の十分性を検証する。
#主要担当者へのインタビューとサイバーセキュリティの実装状況の観察。
質問には「証拠を特定し、目録を入手し、検証する」と具体的に記載されているため、このタスクはフェーズ2：評価の実施に直接該当します。
回答選択肢の内訳
説明
正しい？
A :フェーズ1：評価の計画と準備
#誤り - このフェーズは、証拠収集ではなく、スケジュール、ロジスティクス、計画に焦点を当てています。
B :フェーズ2：評価の実施
#正解 - この段階では、証拠の収集、検証、およびレビューを行います。
C :フェーズ3：推奨評価結果の報告
#誤り - このフェーズでは結果を文書化しますが、証拠は収集しません。
D :フェーズ4：未解決の評価問題の是正
#誤り - このフェーズは、証拠収集ではなく、是正措置に焦点を当てています。
* CMMC評価プロセスガイド（CAP）-フェーズ2：評価の実施には、証拠の収集と検証などのタスクが明確に含まれています。
CMMC 2.0 ドキュメントからの公式参照最終検証と結論正解は B. フェーズ 2: 評価の実施です。このフェーズには、CMMC 準拠を判断するために重要な証拠の特定、取得、検証が含まれます。

最新問題: **132**
C3PAOは、OSCの評価後、限定的な業務上の不備是正評価を完了しました。主任評価者は、不備をPOA&Mに移行することを推奨しましたが、OSCは暫定認証のままとなります。この措置を開始するために、METと評価される必要のある業務の最小数はいくつですか？
A. 80の実践
B. 88の実践
C. 100の実践
D. 110の練習
Answer: C (メーッセージを残す**)**
限定的実践不備修正評価プロセスは、認証取得を目指す組織（OSC）が、認定第三者評価機関（C3PAO）によるCMMCレベル2評価を受け、セキュリティ対策の一部に未解決の不備がある場合に実施されます。
CMMC 2.0 ポリシーおよび DFARS 252.204-7021 によると、OSC は、セキュリティ対策の最低基準を満たし、行動計画およびマイルストーン (POA&M) を通じて不備に対処すれば、暫定認証を取得できます。
* CMMC 2.0 暫定規則では、OSC が POA&M に基づく是正措置を受けるには、110 項目のうち少なくとも 100 項目を満たす必要があると規定されています。

* POA&Mには、後で修正できるように最大10項目の業務内容を記載できます。
* 少なくとも100項目の要件を満たせなかった場合、評価は不合格となり、改善措置を講じた後に再評価を受ける必要があります。
* 主任評価者は、OSCが少なくとも100の診療基準を満たしている場合にのみ、POA&Mの配置を推奨できます。
* METと評価されたプラクティスが100未満の場合、OSCはPOA&Mandの資格を満たさず、完全に再テストを受ける必要があります。
* DFARS 252.204-7021およびCMMC 2.0ポリシーは、条件付き認証の100項目の実施基準を確認しています。
* A. 80回の練習（不正解）100回の練習という要件を大きく下回っています。
* B. 88の診療行為（誤り）- POA&Mの適格基準を下回っています。
* D. 110のプラクティス（誤り）- 110のプラクティスを満たすことが理想的ですが、CMMCでは100のプラクティスでPOA&Mオプションが認められています。
* 正解はCです。100の実践は、POA&Mベースの暫定認証の最低基準を満たしています。
参考文献：
DFARS 252.204-7021（CMMC要件条項）
CMMC 2.0評価プロセス（CAP）ガイド
国防総省CMMC 2.0ポリシー概要

最新問題: **133**
評価プロセスにおいて、利益相反を特定するのはどの段階ですか？
A. 評価を実施する準備ができていることを確認する。
B. 要件を分析する。
C. 最終的な推奨評価結果を生成します。
D. 評価計画を作成する。
Answer: C (メーッセージを残す**)**

最新問題: **134**
OSC（オンタリオ州証券委員会）のレベル2評価が終盤を迎え、最終結果をOSCに提出するための準備が進められています。最終結果はいつOSCに提出すべきでしょうか？
A. 評価の毎日の終わりに
B. 毎日および最終の別日程のレビュー時に
C. 最終日次チェックポイント時、または別途予定されている所見および推奨事項のレビュー時
D. C3PAOの承認後、または別途予定されている最終勧告事項レビューの期間中。
Answer: C (メーッセージを残す**)**
CMMC 2.0 レベル 2 アセスメントにおける報告プロセスの理解 認定第三者評価機関 (C3PAO) が実施する CMMC レベル 2 アセスメントは、証拠の収集、コンプライアンスの評価、および認証取得組織 (OSC) への結果報告について、構造化されたアプローチに従い

ます。報告プロセスは、CMMC アセスメント プロセス (CAP) ガイドに概説されており、結果の伝達方法が規定されています。
毎日のチェックポイント：
評価期間中、評価チームはOSCと毎日チェックポイント会議を開催し、進捗状況、観察事項、および予備的な調査結果について最新情報を提供する。
これらのチェックポイントは透明性を確保するのに役立ち、OSCが軽微な問題が発生した場合に迅速に対処することを可能にする。
最終結果発表：
最終評価結果は通常、毎日の最終チェックポイントで共有されるか、または別途予定された所見と提言のレビュー会議で共有されます。
これにより、公式報告書が提出される前に、OSC（オンタリオ州検察庁）が評価結果の構造化された完全な要約を受け取ることが保証されます。
CMMC評価プロセス（CAP）ガイドのセクション4.5では、評価結果は最終日次チェックポイントまたは別途スケジュールされた最終レビューのいずれかで提示されるべきであると明確に述べられています。
これは、透明性を維持し、最終報告書の提出前にOSCが評価結果を明確に把握できるようにするための最善の慣行に沿ったものです。
オプションA（毎日終了時は、評価者が更新情報を提供するものの、
毎日「最終結果」を発表します。
オプションB（毎日のチェックと別途の最終レビュー）は誤解を招く表現です。CAPガイドでは、評価者は毎日の最終チェックポイントか、別途の所見レビューのどちらかを選択できるのであって、両方を選択できるわけではありません。
選択肢D（C3PAOの承認後）は誤りです。C3PAOは、調査結果がOSCに伝達される前に承認を行うことはありません。評価チームが最初に直接結果を提示します。
CMMC評価プロセス（CAP）ガイド、セクション4.5：報告と結果の伝達 CMMC 2.0レベル2評価プロセスの概要 CMMC評価最終レポートガイドライン 評価コミュニケーション構造 オプションCが正しい理由 公式CMMCドキュメントの参照 最終検証 公式CMMC 2.0ドキュメントに基づくと、最終評価結果は、最後の毎日のチェックポイントまたは別途スケジュールされたレビューセッションでOSCに提示される必要があり、オプションCが正解となります。

最新問題: **135**
CUI（機密情報）の取り扱いを必要とする契約を受注するために、請負業者は最低限どのレベルの認証を取得しなければならないか？
A. レベル1
B. レベル2
C. レベル3
D. どのレベルでも
Answer: B (メーッセージを残す**)**
1. CMMC 2.0レベルとCUI処理要件の理解

CMMC 2.0では、機密指定されていない管理情報（CUI）を取り扱う請負業者は、CUIを含む契約を受注する資格を得るために、最低限の認証レベルを満たさなければならない。
CMMC 2.0 レベル:
レベル1（基礎）- 17の実践
連邦契約情報（FCI）のセキュリティのみを対象としています。
CUI（機密情報）の取り扱い要件を満たしていません。
レベル2（上級）- 110の練習#
CUI（機密情報）の取り扱いに必須です。
CUI（機密情報）を保護するためのセキュリティ管理策を定めたNIST SP 800-171に準拠しています。
CUI（機密情報）の保護を必要とする契約においては、請負業者はレベル2の認証を取得しなければならない。
レベル3（エキスパート）- 110以上の実践例
高額な機密情報（CUI）および国家安全保障上重要な情報に関わる契約に必須。
NIST SP 800-172に基づく追加の保護機能が含まれています。
2. CUIのレベル2を確認する公式CMMC 2.0参照資料
CMMC 2.0モデルの概要には、CUI（機密情報）を取り扱う請負業者にはレベル2が必要であることが明確に記載されています。
DFARS 252.204-7012では、CUIを保護する請負業者は、CMMCレベル2の基礎となるNIST SP 800-171を実装しなければならないと規定しています。
国防総省のレベル2向けCMMC評価ガイドでは、CUI（機密情報）を扱う組織は、契約を獲得するために、NIST SP 800-171に記載されている110項目の実践事項を完全に実施していることを証明する必要があると規定されています。
3. 他の選択肢が間違っている理由
A) レベル1#
FCIのみを対象とし、CUIは対象外です。
Does notmeet DoD requirements for protectingCUI.
C). Level 3#
While Level 3 offersadditional protectionsfor high-risk CUI, it isnot the minimumrequirement.
Level 2 is the minimumneeded to handle CUI.
D). Any level#
OnlyLevel 2 and higherare eligible for contracts requiring CUI protection.
Level 1 doesnotmeet CUI security standards.

最新問題**: 136**
対象となる各ホストユニット、支援組織／ユニット、またはエンクレーブについて、実施基準および関連要素が満たされているかどうかを判断するための証拠の適切性と十分性を検証するのは誰ですか？
A. CSO

B. 評価チーム
C. 権限付与担当者
D. 査定担当者
Answer: B (メーッセージを残す**)**
CMMC評価プロセス（CAP）に基づき、評価チームは評価中に収集された証拠の妥当性と十分性を判断する責任を負います。チームは、対象となる各ホストユニット、サポート組織、またはエンクレーブのプラクティスとコンポーネントが目標とするCMMCレベルを満たしているかどうかを検証します。認証取得組織（OSC）は証拠を提供しますが、検証と採点の決定を行うのは評価チームのみです。
参考資料：
* CMMC評価プロセス（CAP）、v1.0

有効な **CMMC-CCP** 問題集は GoShiken.com が提供された合格しやすい CMMC-CCP 試験問題集！ GoShiken.com が最新の **CMMC-CCP** 試験問題集を提供しています。GoShiken.com CMMC-CCP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CMMC-CCP 問題集をゲットする人はこちら: https://www.goshiken.com/Cyber-AB/CMMC-CCP-mondaishu.html (**23030%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **137**
主任評価者は、OSCのネットワークセキュリティ専門家にインタビューを行った。その月のインシデント監視レポートによると、OSCの外部SOCサービスプロバイダーからセキュリティインシデントは報告されていない。これは、RA.L2-3.11.2 組織のシステムおよびアプリケーションの脆弱性を定期的に、またそれらのシステムおよびアプリケーションに影響を与える新たな脆弱性が特定されたときにスキャンする」の証拠として提供される。この情報に基づき、主任評価者は、証拠が次のとおりであると結論付けるべきである。
A. 実践とは無関係なので不適切です。
B. 想定されるアーティファクトによく適合するため、適切である。
C. セキュリティインシデントの報告がないため、適切です。
D. OSCのサービスプロバイダーにインタビューする必要があるため、不十分です。
Answer: A (メーッセージを残す**)**
RA.L2-3.11.2の理解：脆弱性スキャン
RA.L2-3.11.2の実施基準では、組織に以下のことが求められます。
システムやアプリケーションの脆弱性を定期的にスキャンしてください。
#新たな脆弱性が発見された際にスキャンを実行する。
#脆弱性スキャンツールまたはサービスを使用して、セキュリティ上の弱点を事前に検出します。
インシデント監視レポートが無関係なのはなぜか？

インシデント監視レポートは、セキュリティインシデントを追跡するものであり、脆弱性スキャン活動を追跡するものではありません。
脆弱性スキャンレポートには以下を含める必要があります。
検出された脆弱性の一覧。
#是正措置が講じられました。
#スキャン頻度とスケジュール。
セキュリティインシデントの報告がないことは、脆弱性スキャンが実施されたことを裏付けるものではありません。
正解が「A. 実践とは無関係なので不適切」である理由は？
A) 実践とは無関係なので不適切 # 正解
セキュリティインシデントの報告がないからといって、脆弱性スキャンが実施されたとは限りません。
B) 想定されるアーティファクトによく適合するため適切である #.偽
この制御においては、インシデント監視レポートは想定される成果物ではありません。代わりに、脆弱性スキャンレポートが必要です。
C) セキュリティインシデントが報告されていないため適切である #.偽
インシデントが発生していないからといって、OSCが脆弱性スキャンを実施しているとは限りません。これは有効な証拠にはなりません。
D) OSCのサービスプロバイダーにインタビューする必要があるため不十分です # 誤り プロバイダーにインタビューすることは役立つかもしれませんが、主な問題は、提供された証拠が無関係であることです。
適切な証拠（脆弱性スキャンレポート）が欠落しています。
この回答を裏付けるCMMC 2.0の参考文献：
NIST SP 800-171（要件3.11.2 - 脆弱性スキャン）
定期的に、また新たな脅威が出現した際に、脆弱性をスキャンするという要件を定義します。
CMMCレベル2評価ガイド
RA.L2-3.11.2の証拠には、インシデント監視レポートではなく、脆弱性スキャンレポートを含めるべきであると規定している。
CMMC 2.0モデルの概要
組織は、インシデント検出だけに頼るのではなく、スキャンを通じて脆弱性を積極的に特定する必要があることを確認する。

最新問題: **138**
CMMC準備状況レビューにおいて、OSCは関連するエンクレーブをレビュー対象範囲から除外すべきであると提案しました。この要求を検証する責任は誰にありますか？
A. 中国共産党
B. C3PAO
C. 主任評価者
D. 諮問委員会

Answer: (解答を表示する**)**
CMMC認証取得準備状況審査において、認証取得希望組織（OSC）は、特定のエンクレーブ（ネットワークセグメントまたはシステム）が評価対象外であると主張する場合があります。主任審査官は、この要求を検証し承認する責任を負います。
CMMC評価における役割と責任：
CMMC認定プロフェッショナル（CCP）
CCPはOSCが評価の準備を行うのを支援するが、最終的な範囲決定は行わない。
認定第三者評価機関（C3PAO）
C3PAOは評価を監督するが、評価範囲の除外事項を個人的に検証することはない。それは主任評価者の役割である。
主任評価者（正解）
主任評価官は、OSCから提供された証拠に基づいて、飛び地が評価対象範囲外であるかどうかを判断する権限を有する。
主任評価者は、適切な範囲設定を確実にするために、CMMC評価プロセス（CAP）のガイドラインに従います。
諮問委員会
CMMC諮問委員会（CMMC-AB）は、適用範囲の決定は行いません。プログラムの監督と認証プロセスに重点を置いています。
正解を裏付ける公式資料：
CMMC評価プロセス（CAP）v1.0
主任評価者は、評価範囲を確認し、対象区域の適用可能性を判断する責任を負います。
CMMCレベル2評価に関する範囲設定ガイドライン
主任評価者は、評価範囲を確定する前に、飛び地除外事項を確認し承認する必要がある。
結論：
リードアセッサーが正解です。なぜなら、リードアセッサーは評価中に範囲決定を検証する権限を持っているからです。

最新問題**: 139**
CMMCのスコープは、CUIが存在する場所に焦点を当てたシステム、アプリケーション、サービスを含むCUI環境を対象としています。
A. 受信および転送。
B. 保存、処理、送信。
C. 入力、編集、操作、印刷、閲覧。
D. 電子媒体、システムコンポーネントのメモリ、および紙媒体に存在する。
Answer: B (メーッセージを残す**)**
CMMCレベル2のスコープガイドでは、CUI資産には、管理対象非機密情報（CUI）を保存、処理、または送信するシステム、アプリケーション、およびサービスが含まれると概説しています。これらは、認証取得を目指す組織（OSC）におけるCUIの取り扱いを定義する3つの主要機能です。
段階的な解説 #1. CMMCで定義されているCUI資産

* 保存場所: CUI はハードドライブ、クラウドストレージ、またはデータベースに保存されます。
* 処理済み: CUI は、アプリケーションやユーザーによって積極的に使用、変更、または分析されています。
* 送信: CUI は、電子メール、ファイル転送、またはネットワーク通信を介してシステム間で送信されます。
#2. 他の選択肢が間違っている理由：
* (A) 受領および転送#
* CUIの受領と転送はCUIの取り扱いの一部ではありますが、CUI資産に関するすべての責任を完全に網羅するものではありません。
* (C) 入力、編集、操作、印刷、閲覧#
* これらは処理内の特定のアクションですが、CMMC のスコープ設定に必要なストレージや送信は含まれません。
* (D) 電子媒体、システムコンポーネントメモリ、および紙媒体#に記録されている
* CUIは電子形式と物理形式の両方で存在し得るが、CMMCのスコープは、CUIが物理的に存在する場所ではなく、CUIがどのように積極的に管理されるか（保存、処理、送信）に焦点を当てている。
* CMMCレベル2スコープガイドでは、CUI資産はCUIの保存、処理、または送信における役割に基づいて分類されることが確認されています。
* NIST SP 800-171でも、これら3つの機能をCUI保護の重要な構成要素として定義しています。
CMMCドキュメントに基づく最終検証：

最新問題: **140**
請負業者は、入札要項に指定されたレベルのCMMC認証を取得することがいつ義務付けられますか？
A. 募集提出時
B. 受賞時
C. 提出期限前
D. 受賞日から30日以内
Answer: B (メーッセージを残す**)**

最新問題: **141**
特定の診療行為に関する証拠の出典を特定する上で、最も適切な資料はどれですか？
A. NISTSP 800-53
B. NISTSP 800-53A
C. CMMC評価範囲
D. CMMC評価ガイド
Answer: D (メーッセージを残す**)**

CMMC評価ガイドは、特定のプラクティスに関するエビデンスの出典を特定する上で最適な情報源です。なぜなら、組織がCMMCプラクティスをどのように実装し、準拠を実証すべきかについて具体的なガイダンスを提供しているからです。CMMCの各レベルにはそれぞれ独自の評価ガイド（例CMMC評価ガイド - レベル1、レベル2）があり、期待されるエビデンスと評価手順が詳細に記載されています。
詳細な正当化理由：
CMMC評価ガイド（証拠の主要情報源）
CMMC評価ガイドでは、各実践事項への準拠を確認するために必要な証拠が明確に示されています。
本書は評価目標に関する詳細な指示を提供し、評価者がコンプライアンスを判断する際に何に着目すべきかを明確にしている。
このガイドでは、各実践項目を評価目標に細分化し、組織が適切な文書や成果物を準備できるよう支援します。
その他の文書と、それらが最良の選択肢ではない理由：
NIST SP 800-53（オプションA）
NIST SP 800-53はセキュリティとプライバシーに関する包括的な管理策のカタログを提供しているが、CMMC固有の証拠要件には焦点を当てていない。
これはサイバーセキュリティの基礎となるフレームワークとして機能するが、CMMC評価に必要な具体的な成果物を定義するものではない。
NIST SP 800-53A（オプションB）
NIST SP 800-53Aはセキュリティ制御の評価に関するガイダンスを提供するが、CMMCフレームワークに特化したものではない。
これには一般的な管理評価手順が含まれていますが、CMMC評価ガイドはCMMC準拠に必要な証拠をより具体的に定義しています。
CMMC評価範囲（オプションC）
CMMC評価範囲文書では、評価の対象となるシステム、資産、およびプロセスについて概説しています。
境界線を明確にする上で重要ではあるものの、各実践における具体的な証拠要件に関する詳細は提供していない。
CMMC公式文書からの引用：
CMMC評価ガイド（レベル2）- 「評価目標」のセクション
この文書では、CMMCの各実践における証拠の収集方法と評価方法について詳述します。
例：AC.L2-3.1.1（アクセス制御 - システムアクセスの制限）の場合、ガイドでは、評価者は文書化されたポリシー、システム構成、および監査ログを確認する必要があると規定されています。
CMMCモデルの概要（米国国防総省公式文書）
CMMC評価ガイドは、証拠の出典を特定するための公式な参考資料であることを強調する。
結論：

CMMC評価ガイドは、CMMC評価における特定のプラクティスに必要な証拠を判断するための最も権威ある情報源です。評価の目的、必要な成果物、およびコンプライアンスに必要な検証手順について、詳細な内訳を提供します。

最新問題: **142**
CMMCレベル1の自己評価で、OSCの施設内にFCIを処理、保管、送信しない資産が特定されました。これはどのタイプの資産とみなされますか？
A. 対象外資産
B. 政府発行資産
C. FCIアセット
D. 特殊資産
Answer: A (メーッセージを残す**)**

最新問題: **143**
CMMCのレベル1の実践記述は 基礎」です。では、レベル2の実践記述とは何ですか？
A. 専門家
B. 上級
C. 最適化
D. 継続的に改善
Answer: B (メーッセージを残す**)**
CMMC 2.0のレベルとその説明を理解するサイバーセキュリティ成熟度モデル認証（CMMC）2.0は、サイバーセキュリティの成熟度の向上を表す3つのレベルで構成されています。
レベル1 - 基礎
基本的なサイバー衛生に焦点を当てる
FAR 52.204-21に準拠した17の慣行を実施
主に連邦政府契約情報（FCI）を保護します。
レベル2 - 上級（正解）
機密指定されていない管理情報（CUI）の保護に重点を置いています。
NIST SP 800-171に準拠した110のプラクティスを実装
重要なプログラムについては、3年ごとの第三者機関による評価を義務付ける。
レベル3 - エキスパート
APT（高度持続的脅威）に対する高度なサイバーセキュリティに重点を置き、NIST SP 800-171および追加のNIST SP 800-172コントロールを実装し、3年ごとの政府主導の評価を要求します。CMMC 2.0フレームワークでは、レベル2が 高度」と明示的に記述されています。NIST SP 800-171に準拠し、堅牢なCUI保護を保証します。
A) エキスパート（不正解）- これはレベル3の説明であり、レベル2の説明ではありません。
C). 最適化（誤り）- 定義されていないCMMCレベルの記述です。
D) 継続的改善 (誤り) - CMMC ではこの用語は使用されません。
正解はB. 上級で、これはCMMCレベル2を正確に表しています。

参考文献：
CMMC 2.0モデルの概要
CMMC 2.0 スコープガイド
NIST SP 800-171 および NIST SP 800-172

最新問題**: 144**
Which authority leads the CMMC direction, standards, best practices, and knowledge framework for how to map the controls and processes across different Levels that range from basic cyber hygiene to advanced cyber practices?
A. DoD CIO office
B. NIST
C. Federal CIO office
D. Defense Federal Acquisition Regulation Council
Answer: A (メーッセージを残す**)**

最新問題**: 145**
CMMCレベル2評価の計画段階において、主任評価者は各実践事項について適切な証拠とは何かを検討します。評価者は何を検証しようとしているのでしょうか？
A. 適切性
B. 十分性
C. プロセスマッピング
D. 評価範囲
Answer: (解答を表示する**)**
CMMCレベル2評価における証拠の十分性の理解CMMCレベル2評価では、主任評価者は、各実践について収集された証拠が評価結果を裏付けるのに十分であるかどうかを判断する必要があります。これは、評価者が以下を評価することを要求するCMMC評価プロセス（CAP）ガイドに準拠しています。
検査 - 文書、構成、およびシステム記録のレビュー。
インタビュー：担当者と面談し、実施状況と理解度を確認する。
テスト :セキュリティ対策が実際に機能している様子を観察し、その有効性を検証する。
証拠が十分かどうかを判断するために、評価者は以下の点を確認します。
評価目標を直接的に支援する。
この慣行が一貫して実施されていることを示す。
独自に検証可能である。
十分性とは、法令遵守について正確な判断を下すのに十分な証拠が収集されているかどうかを指します。
選択肢A（妥当性）は誤りです。妥当性とは証拠の質に関することですが、十分性とは十分な証拠が存在するかどうかに関することです。
選択肢C（プロセス・マッピング）は誤りです。プロセス・マッピングはワークフローを理解するために使用されますが、評価検証方法ではありません。

選択肢D（評価範囲）は誤りです。なぜなら、評価範囲の定義は証拠収集の前に、計画段階で行われるからです。
CMMC評価プロセス（CAP）ガイド - セクション3.6（証拠の十分性の決定）CMMCレベル2評価ガイド - 証拠の収集と評価 オプションB（十分性）が正しい理由 公式CMMC文書参照 最終検証 主任評価者がコンプライアンスを確認するために十分な証拠が利用可能であることを確認しているため、正解はオプションB：十分性です。

最新問題: **146**
ある企業がプレスリリースを発表しようとしています。AC.L1-3.1.22「公開アクセス可能なシステムに掲載または処理される情報の管理」によると、CMMC要件に対応する際に考慮すべき最も重要な要素は何ですか？
A. 情報が正しい
B. CEOがそのメッセージを承認した
C. 会社はFCIの放出を保護しなければならない
D. FCIの情報のみであれば公開できる
Answer: C (メーッセージを残す)
* AC.L1-3.1.22には、「公開アクセス可能なシステムに掲載または処理される情報を制御する」と記載されています。
* この規制では、組織はFCI（連邦契約情報）が公に公開されたり、管理されていない方法でアクセス可能になったりしないようにする必要があります。
* FCIは、機密情報やCUIではない場合でも、不正な開示から保護されなければならない。
参照：
NIST SP 800-171、要件3.1.22
CMMCレベル1実践AC.L1-3.1.22
ステップ 2: プレスリリースで FCI を保護することが重要な理由 企業が FCI を含むプレスリリースを発表する場合、その情報が意図せず機密性の高い契約関連データを公開しないようにする必要があります。
FCIには、国防総省が契約に基づいて提供または作成した情報が含まれますが、これらの情報は一般公開を目的としていません。
組織は、意図しない暴露を防ぐための管理策を実施しなければならない。
ステップ3：他の選択肢が間違っている理由A. 情報が正しい（間違い）：
正確性も重要ですが、CMMCの要件は、単に正確性を確保するだけでなく、機密情報を保護することに重点を置いています。
B :CEOがそのメッセージを承認した（誤り）：
CEOの承認は、FCIの保護に対応していないため、CMMC準拠を満たしません。
D: 情報がFCIのみである限り、公開できる（誤り）
FCIは保護されるべきものであり、国防総省による特別な許可がない限り、公に開示してはならない。

正解の最終確認：会社はFCIを保護し、公式プレスリリースにおいて不正な情報開示が行われないようにしなければならない。
したがって、正解はCです。会社はFCIの放出を保護しなければなりません。

最新問題: **147**
According to DFARS clause 252.204-7012, who is responsible for determining that Information in a given category should be considered CUI?
A. The NARA CUI Executive Agent
B. The contractor who generated the information
C. The DoD agency for whom the contractor is performing the work
D. The military personnel assigned to the contractor for that purpose
Answer: (解答を表示する**)**
DFARS clause 252.204-7012 establishes the safeguarding of Covered Defense Information (CDI), which aligns with CUI categories. The clause specifies that the DoD is responsible for determining whether information is Controlled Unclassified Information (CUI) and marking it accordingly before sharing it with contractors. Contractors do not make determinations about what constitutes CUI; they are responsible for safeguarding information once it is received and marked as CUI.
Reference Documents:
* DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting
* CMMC Model v2.0 Overview, December 2021

最新問題: **148**
CMMCレベル2認証評価後、主任評価者（主任CA）は最終推奨事項をOSCに提示する準備をしています。主任評価者が評価結果をOSCに提出する責任を最も適切に説明しているのは、次のうちどれですか？
A. CMMC評価結果概要書を用いて提示された要約勧告で十分です。
B. 詳細な調査結果は、評価が評価者の調査結果とどのように対応しているかを明確に示す証拠とともに、OSCに提出されなければなりません。
C. OSCに提出される最初のレポートには、全体的な評価の「MET」または「NOT MET」のスコアと、各プラクティスのスコアのみが含まれます。
D. 主任評価者は、OSCと共有する前に、最初の評価結果をC3PAOに提出して審査を受ける必要があります。
Answer: D (メーッセージを残す**)**
CMMC評価プロセス（CAP）v2.0では、評価結果を「初期」または未検証の所見としてOSCに提出することは想定されていません。代わりに、CAP v2.0では、C3PAOがOSCとのアウトブリーフィング会議の前に、認証評価結果の正式な品質保証（QA）レビューを実施することが求められています。このQA手順は必須であり、結果をOSCに伝える前に明確に順序付けられています。

結果がまとめられ、品質レビューが行われた後、リードCCAは「評価結果をOSCに伝える」ためにアウトブリーフィング会議を招集します。CAP v2.0ではさらに、チームがアウトブリーフィングのために「評価結果ブリーフィング」を準備して発表することが求められており、必要な内容（各セキュリティ要件に対する最終的なMET/NOT MET/NAの判定、POAおよびMのステータス（該当する場合）、証明書の判定など）がリストされています。
したがって、CAP v2.0では、アウトブリーフィング中にOSCに正式に提示される前に、結果はC3PAOの品質保証レビューを受けなければならないことが明確に規定されているため、Dが最適な答えです。

最新問題: **149**
CMMCエコシステムにおいて、最終的にどの組織が候補者評価者およびインストラクターのトレーニング、テスト、承認、および認定を管理・監督するのでしょうか？
A. 国防総省国防次官補
B. DIB共同情報共有環境
C. 国家安全保障システム委員会指示
D. CMMC評価者およびインストラクター認定機関
Answer: (解答を表示する**)**
CMMCエコシステムにおけるCAICOの役割を理解する
CMMCエコシステムは、サイバーセキュリティ成熟度モデル認証（CMMC）プログラムのさまざまな側面を管理、実装、監督する複数の組織で構成されています。
主要な組織の一つは、CMMC評価者およびインストラクター認定組織（CAICO）であり、以下の責任を負っています。
評価者および指導者の研修と認定。
CMMC専門家向けのテスト、承認、および認証の管理。
評価担当者が資格およびコンプライアンス基準を満たしていることを確認する。
選択肢D（CAICO）が正解である理由
CAICOは、評価者およびインストラクター候補者の訓練、試験、承認、および認定を明確に任務としている。
選択肢A（国防次官室）は誤りです。国防次官室（OUSD）は政策監督は行いますが、評価者の認定は行いません。
オプションB（DIB共同情報共有環境）は、DIB CISが防衛産業基盤内での情報共有に焦点を当てており、評価者の認証に焦点を当てていないため、誤りです。
選択肢C（国家安全保障システム委員会の指示）は誤りです。CNSSIはセキュリティ基準を提供するだけで、評価者のトレーニングや認証を管理しているわけではないからです。
CMMC公式ドキュメントの参照
CMMCエコシステムの概要 - CAICOの役割
CMMC評価プロセス（CAP）ガイド - 評価者認定およびトレーニング最終検証 CAICOはCMMC評価者およびインストラクターのトレーニング、テスト、および認定を担当しているため、正解はオプションD：CMMC評価者およびインストラクター認定組織です。

最新問題: **150**
証拠の記録が適切であるとは、以下の基準を満たす必要があると定義されます。
A. 評価と組織範囲に基づいて検証します。
B. 評価と組織的実践に基づいて検証する。
C. 与えられた成果物、インタビューの回答、デモンストレーション、またはテストがCMMCの範囲を満たしているかどうかを判断します。
D. 与えられた成果物、インタビューの回答、デモンストレーション、またはテストがCMMCの実践を満たしているかどうかを判断します。
Answer: D (メーッセージを残す)
CMMC評価プロセスにおける「適切な証拠」の理解CMMC評価において、適切な証拠とは、特定のサイバーセキュリティ対策が正しく実施されていることを証明するために必要な証拠を指します。証拠は以下から得られます。
* アーティファクト（例セキュリティポリシー、システム構成、ログ）。
* インタビューでの回答（例：担当者の職務内容に関する口頭での確認）。
* デモンストレーション（例セキュリティ制御がリアルタイムでどのように実装されるかを示す）。
* テスト（例：多要素認証などの技術的なセキュリティメカニズムの検証）。
証拠収集の目的は、組織が評価範囲内で運営されているかどうかだけでなく、CMMCの実施基準を満たしているかどうかを判断することです。
* A. 評価と組織範囲に基づいて検証する # 不正解
* 評価範囲は評価対象を定義しますが、証拠の妥当性は特定のCMMCの慣行への準拠に基づいています。
* B. 評価と組織慣行に基づいて検証する # 不正解
* CMMC評価は、一般的な組織慣行だけでなく、CMMCフレームワークで定義されているサイバーセキュリティ対策に焦点を当てています。
* C. 与えられた成果物、インタビュー回答、デモンストレーション、またはテストがCMMCの範囲を満たしているかどうかを判断する # 不正解
* スコープは評価の範囲を定義しますが、評価チームの役割はCMMCの実践が満たされているかどうかを確認することです。
* D. 与えられた成果物、インタビュー回答、デモンストレーション、またはテストがCMMCの実践基準を満たしているかどうかを判断する # 正解
* CMMCの評価プロセスは、必要な対策が実施されていることを確認することに重点を置いているため、これが正解です。
正解が「与えられた成果物、インタビューの回答、デモンストレーション、またはテストがCMMCの実践基準を満たしているかどうかを判断する」（D）である理由は？
* CMMC評価プロセス（CAP）文書
* 「十分な証拠」とは、CMMCの実施が正しく行われたことの証明と定義する。
* CMMC 2.0評価基準

* 証拠は特定のサイバーセキュリティ対策に照らして評価されなければならないことを規定する。
* NIST SP 800-171A（NIST SP 800-171の評価手順）
* 必要な手順への準拠を確認するために、成果物、インタビュー、デモンストレーション、およびテストを評価する際のガイダンスを提供します。
この回答を裏付けるCMMC 2.0の参考文献：
最終回答:#D. 与えられた成果物、インタビュー回答、デモンストレーション、またはテストがCMMCの実践基準を満たしているかどうかを判断します。

最新問題: **151**
防衛関連企業はFCIを下請け業者と共有する必要があり、このデータを電子メールで送信します。このプロセスで使用される電子メールシステムは以下の目的で使用されます。
A. FCIを管理する。
B. FCIプロセス。
C. FCIを送信します。
D. FCIを生成する
Answer: C (メーッセージを残す**)**
連邦契約情報（FCI）は、FAR 52.204-21において、契約に基づき政府によって提供または生成された情報であって、一般公開を目的としない情報と定義されています。CMMC 2.0の下では、FCIを取り扱う組織は、FAR 52.204-21の基本保護要件を実装し、FCIの処理、保管、および送信において適切な保護を確保する必要があります。
与えられた選択肢の分析この問題は、FCIを下請け業者に送信するために使用される電子メールシステムに関するものです。
考えられる答えを詳しく見ていきましょう。
A). FCI# の管理が正しくありません
FCIの管理には、FCIの整理、保管、アクセス維持といった活動が含まれます。電子メールの送信は管理には含まれません。それは単なる送信行為です。
B). プロセスFCI#が正しくありません
処理とは、データの分析、変更、計算など、運用上または分析上の目的でFCIを積極的に使用することを指します。単にメールを送信するだけでは、処理には該当しません。
C). FCI# 正しい値を送信してください
送信とは、FCIをある組織から別の組織へ送信する行為を指します。請負業者はFCIを電子メールで送信しているため、これはデータの送信に該当します。
参照:NIST SP 800-171 Rev. 2、3.1.3- 承認されたメカニズムを使用して送信することにより、CUI またはFCI）を制御する。」D) FCI# の生成 誤り FCI の生成とは、新しい契約関連情報を作成することを意味します。このシナリオでは、請負業者は FCI を作成しているのではなく、単に送信しているだけです。
正解を裏付ける公式資料 :CMMC 2.0 レベル1の実施基準（FAR 52.204-21 基本的安全対策管理）

3.1.3：承認されたメカニズムを使用してCUI（またはFCI）を送信することにより、CUI（またはFCI）を制御する。」これは、電子メールの送信がFCIの「送信」に該当し、管理や処理には該当しないことを確認するものです。
NIST SP 800-171 Rev. 2（非連邦システムにおけるCUIの保護）
要件3.13.8：「CUIを送信する際に暗号化方式で保護する。」これは主にCUIに適用されますが、FCIも送信中に保護されるべきであり、電子メールが情報伝送の一形態であることを確認します。
結論：請負業者はFCIを電子メールで送信しているため、正解はC. FCIを送信することです。これは、送信データのセキュリティを重視するFAR 52.204-21およびNIST SP 800-171に基づくCMMC 2.0レベル1の慣行と一致しています。

有効な **CMMC-CCP** 問題集は GoShiken.com が提供された合格しやすい CMMC-CCP 試験問題集！ GoShiken.com が最新の **CMMC-CCP** 試験問題集を提供しています。GoShiken.com CMMC-CCP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CMMC-CCP 問題集をゲットする人はこちら: https://www.goshiken.com/Cyber-AB/CMMC-CCP-mondaishu.html (**23030%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **152**
CMMC-ABの職業倫理規定を定義する際に、どのような原則が含まれていますか？
A. 客観性、分類、および情報の正確性
B. 客観性、機密性、および情報の完全性
C. 責任、分類、および情報の正確性
D. 責任、機密保持、および情報保全
Answer: (解答を表示する**)**
CMMC-AB 専門職行動規範の理解サイバーセキュリティ成熟度モデル認証認定機関 (CMMC-AB) (現在は Cyber AB と呼ばれています) は、認定評価者 (CA)、認定専門家 (CP)、および C3PAO (認定第三者評価機関) を含む、CMMC 評価に関わるすべての個人のための専門職行動規範 (CoPC) を定めています。
CMMC-ABの職業倫理規定に概説されている中核的な原則は以下のとおりです。
責任
CMMCの専門家は、自らの行動に全責任を負い、評価が誠実かつ専門的に実施されることを保証しなければならない。
彼らは、サイバーABおよび国防総省によって定められたすべての倫理的および規制上の要件を遵守しなければならない。
機密保持
CMMCの専門家は、機密情報（CUIおよびFCIを含む）を保護しなければなりません。

彼らは秘密保持契約（NDA）を遵守し、不適切な情報共有を避けることが求められる。
情報整合性
CMMC評価におけるすべての報告書、調査結果、および勧告は、正確かつ偏りのない真実でなければならない。
評価者は利益相反を避け、評価において提供されるすべてのデータが検証可能であり、虚偽表示がないことを保証しなければならない。
回答A（不正解）CMMC-AB CoPCの主要原則は「分類」ではありません。重点は分類手順ではなく、CUIとFCIの保護に置かれています。
解答B（不正解）：客観性は重要ですが、CMMC-AB専門職倫理規定の3つの基本原則の1つとして明示的に挙げられていません。
解答C（不正解）「分類」はCoPCの指導原則ではありません。
正解はDです。職業倫理規定では、責任、機密保持、および情報の完全性を明確に強調しています。
正解はDです。責任、機密保持、および情報保全。
これらの原則は、すべてのCMMC専門家が倫理基準を維持し、認証プロセスの完全性を守ることを保証するものです。
参考文献：
CMMC-AB 専門職倫理規定 (CoPC)
サイバーAB倫理ガイドライン
CMMC評価プロセス（CAP）ガイド

最新問題: **153**
OSCのCMMC評価を開始する前に、主任評価者は評価の最も重要な要件についてチームに説明しました。評価者はまた、調査結果の概要、実践評価、およびレベル推奨事項の同じ結果を、初期プロセスとレビューのためにC3PAOに提出する必要があると主張しました。数週間の評価の後、C3PAOは内部レビューを完了し、推奨された結果は最終的な品質レビューと評価承認のためにC3PAOを通じて提出されます。これらの報告要件を規定している文書はどれですか？
A. CMMC評価報告要件
B. DFARS 52.204-21 評価報告要件
C. NISTSP 800-171 改訂版2 評価報告要件
D. DFARS条項252.204-7012評価報告要件
Answer: (解答を表示する**)**
正解はAです。CMMC評価報告要件。この文書は、認定第三者評価機関（C3PAO）がCMMC評価を実施および報告する際に従うべき構造化されたプロセスを具体的に概説しているからです。
手順ごとの詳細：
CMMC評価プロセスを理解する
主任評価者は、評価開始前にチームに対し、評価要件と評価基準について説明します。

評価全体を通して、調査結果の概要、実践評価、およびレベルに関する推奨事項が文書化され、報告されます。
これらの調査結果は、正式に品質審査および最終評価承認のために提出される前に、C3PAOによって内部的に審査されます。
報告要件を規定する主要文書：CMMC評価報告要件 この文書では、CMMCエコシステム内で評価をどのように報告する必要があるかを具体的に詳述しています。
これは、組織が最終的な認証決定を受ける前に、評価の提出、内部C3PAOによるレビュー、およびCMMC-ABによる品質チェックを行うための構造化されたプロセスを説明するものです。
これにより、結果の一貫性、透明性、および国防総省のサイバーセキュリティコンプライアンス要件との整合性が確保されます。
他の選択肢が間違っている理由：
B) DFARS 52.204-21 評価報告要件
This clause only specifiesbasic safeguardingof Federal Contract Information (FCI) but doesnotdictate the reporting process for CMMC assessments.
C). NIST SP 800-171 Revision 2 Assessment Reporting Requirements
WhileNIST SP 800-171 Rev. 2outlines security controls, it doesnotdefine how CMMC assessments must be conducted and reported.
D). DFARS Clause 252.204-7012 Assessment Reporting Requirements
This DFARS clause focuses onincident reportingandcyber incident response requirementsbut does not detail theCMMC assessment reporting process.
Official Reference:
CMMC Assessment Reporting Requirements, issued byThe Cyber ABandDoD, governs how C3PAOs must report assessment results.
CMMC Assessment Process (CAP)also outlines reporting workflows for certification.
Thus, theCMMC Assessment Reporting Requirementsdocument is the authoritative source that dictates the reporting procedures for CMMC assessments.

最新問題**: 154**
請負業者は国防総省にサービスとデータを提供します。FCI（連邦契約情報の処理に必要なトランザクションは請負業者の社内ネットワーク上で行われますが、作業は請負業者所有のシステム上で実行されます。これらのシステムは政府の要件に基づいて構成され、契約をサポートするために使用されます。これらのシステムはどのような種類の特殊資産に該当しますか？
A. たくさん
B. 制限付きIS
C. 試験装置
D. 政府所有物
Answer: B (メーッセージを残す**)**
CMMCスコープにおける制限情報システム（IS）の理解

CMMC 2.0では、特殊資産とは、従来のITシステムカテゴリには当てはまらないものの、連邦契約情報（FCI）または管理対象非機密情報（CUI）の処理、保存、または送信において役割を果たす資産を指します。CMMCスコープガイドにおける特殊資産の4つのカテゴリは以下のとおりです。
モノのインターネット（IoT）デバイス - スマートデバイスまたはネットワーク接続デバイス。
制限情報システム（制限IS）ー契約上、政府の仕様に合わせて構成することが義務付けられているシステム。
試験装置 - 特殊な試験や測定に使用される機器。
政府所有物 - 米国政府が所有するが、請負業者が使用する機器。
B. 制限付きIS」が正しいのはなぜですか？
問題となっている請負業者所有のシステムは、政府の要件に基づいて構成されており、国防総省との契約を支援するために使用されている。
制限付き情報資産は、契約上、政府のセキュリティ要件を満たし、国防総省関連の情報を扱うことが義務付けられています。
これらのシステムは一般的なIT資産には該当せず、特別な取り扱いが必要となるため、CMMCスコープガイドによれば制限付き情報システム（Restricted IS）に分類されます。
他の回答が間違っている理由とは？
A) IoT（不正解）
IoTデバイスにはスマートデバイス、センサー、組み込みシステムなどが含まれますが、請負業者の業務システムはIoTには分類されません。
C）試験装置（不正解）
請負業者のシステムはFCIの処理に使用されるものであり、試験や測定に使用されるものではありません。
D）政府所有物（誤）
これらのシステムは請負業者が所有しており、米国政府が所有しているものではないため、政府資産には該当しません。
結論
正解はBです。制限付き情報システム（IS）です。システムは請負業者が所有していますが、国防総省のセキュリティ要件に従う必要があります。
参考文献：
CMMC 2.0 レベル2 スコープガイド
国防総省CMMCポリシーおよびDFARS 252.204-7012

最新問題: **155**
主任評価者は、レベル2評価を完了するために必要なすべての作業が完了していることを確認します。最終的な評価結果パッケージは適切にレビューされ、アップロードの準備が整いました。主任評価者は、他にどのような資料の維持管理と保護を担当するのでしょうか？
A. 評価に関する追加のメモや情報

B. C3PAOによる最終評価計画書および品質管理報告書
C. 最終評価計画書、および主任評価者による評価プロセスの説明書簡
D. 最終評価計画書、主任評価者による結果説明書簡、およびC3PAOからの品質管理報告書
Answer: A (メーッセージを残す**)**
主任評価者は、評価プロセス中に収集されたすべての評価記録、メモ、および情報を保護および維持する責任を負います。これには、監査や紛争解決のために必要となる可能性のある作業書類や補足資料も含まれます。
公式コンテンツからの補足抜粋：
* CAP v2.0、評価後の責任（§3.17）：主任評価者は、すべての評価成果物、メモ、および情報がC3PAOの方針に従ってアーカイブまたは廃棄されていることを確認しなければならない。」オプションAが正しい理由：
* CAPでは、評価に関するメモや情報は、規定に従って保存または廃棄しなければならないと規定されています。
* オプションB、C、Dは、CAPで必須ではない項目です。「手紙」と「品質管理レポート」は、主任評価者が保管する必要のある資料には含まれません。
参考文献（CMMC v2.0公式コンテンツ）：
* CMMC評価プロセス（CAP）v2.0、フェーズ3事後評価（§3.17）。

最新問題**: 156**
レベル1の自己評価中に、スマートサーモスタットが検出されました。これはOSCのWiFiネットワークでインターネットに接続されています。これはどのような種類の資産ですか？
A. FCIアセット
B. CUI資産
C. 対象資産
D. 特殊資産
Answer: D (メーッセージを残す**)**
CMMC 2.0における資産分類の理解
CMMC 2.0では、資産は、その機能、接続性、および連邦契約情報（FCI）または管理対象非機密情報（CUI）を処理、保存、または送信するかどうかに基づいて、異なるタイプに分類されます。
D. 特殊資産」が正しい理由とは？
CMMC 2.0 スコープガイドでは、特殊資産を、従来の IT 分類には当てはまらないが、組織環境内に存在する資産と定義しています。
スマートサーモスタットは、CMMCで定義されている特殊資産に分類されるモノのインターネット（IoT）デバイスです。
他の回答が間違っている理由とは？
A) FCI資産（誤）

FCI Assetsは、スマートサーモスタットとは異なり、連邦契約情報を処理、保存、または送信しません。
B). CUI資産（誤り）
CUIアセットは管理対象非機密情報を取り扱いますが、athermostatはCUIを処理しません。
C) 対象範囲内の資産（誤り）
対象となる資産にはFCI資産とCUI資産が含まれますが、スマートサーモスタットはこれらには該当しません。
結論
正解はDです。スマートサーモスタットはIoTデバイスであり、特殊資産のカテゴリに分類されます。
参考文献：
CMMC 2.0 スコープガイド
米国防総省のIoTデバイスに関するサイバーセキュリティガイドライン

最新問題: **157**
CMMC-ABの職業倫理規定を定義する際に、どのような原則が含まれていますか？
A. 客観性、分類、および情報の正確性
B. 客観性、機密性、および情報の完全性
C. 責任、分類、および情報の正確性
D. 責任、機密保持、および情報保全
Answer: D (メーッセージを残す**)**
Cyber AB（旧CMMC-AB）の専門職行動規範（CoPC）は、CMMCエコシステムに関わるすべてのメンバー（認定CMMCプロフェッショナル（CCP）および認定CMMCアセッサー（CCA）を含む）が遵守しなければならない義務的な規約です。この規範は、評価プロセスの信頼性と確実性を保証するものです。
CoPCの基盤を形成する基本原則は以下のとおりです。
責任：これは、CMMC専門家がCMMCプログラム、国防総省（DoD）、および国民の最善の利益のために行動する義務を指します。これには、専門能力の維持と、職務を適切な注意を払って遂行することが含まれます。
機密保持：評価者および専門家は、機密情報（管理非機密情報CUI）や認証申請組織（OSC）の専有ビジネスデータなど）へのアクセスを許可されています。彼らは、これらの情報が不正に開示されないよう保護しなければなりません。
情報の完全性：この原則は、評価中に生成されるすべてのデータ、調査結果、および報告書が正確かつ完全であり、改ざんされていないことを要求するものです。これにより、「達成」または「未達成」の判断が、誠実な証拠に基づいていることが保証されます。
他の選択肢が間違っている理由：
オプションAとB（客観性）：評価者にとって「客観性」は重要な行動要件（偏りを持たずにいること）ですが、CMMCプロフェッショナル研修や正式なCoPC文書で強調される具体的な

高レベルの三位一体は、標準的な職業倫理と情報セキュリティの柱に沿うように、責任機密性完全性のフレームワークに焦点を当てています。
オプションAとC（分類） 「分類」は国家安全保障情報（機密情報）に使用されるプロセスですが、CMMCは主に非機密情報（CUIおよびFCI）に焦点を当てています。
分類は、専門職倫理規定の中核となる原則ではない。
オプションAとC（情報の正確性）：正確性は非常に重要ですが、CCPカリキュラムで提供される正式な定義では、情報の完全性の一部とみなされています。
参考資料：
CMMC-AB（サイバーAB）専門職行動規範：資格を有するすべての個人に適用される公式の倫理的枠組み。
CMMCプロフェッショナル（CCP）学習ガイド：「倫理と職業行動規範」のセクション。CMMC評価プロセス（CAP）：評価エコシステムの完全性を維持するために必要な倫理基準を参照しています。

最新問題: **158**
Which organization is the governmental authority responsible for identifying and marking CUI?
A. NARA
B. Department of Homeland Security
C. NIST
D. CMMC-AB
Answer: (解答を表示する**)**

最新問題: **159**
情報、関連する情報処理サービス、および特定の物理的施設への立ち入りに関する特定の要求を許可または拒否するプロセスを表す用語はどれですか？
A. アクセス制御
B. 物理的なアクセス制御
C. 強制アクセス制御
D. 任意アクセス制御
Answer: A (メーッセージを残す**)**
CMMCにおけるアクセス制御の理解アクセス制御とは、特定の要求を許可または拒否するプロセスを指します。
* 情報の入手と利用
* アクセス情報処理サービス
* 具体的な場所を入力してください
CMMCのアクセス制御（AC）ドメインは、NIST SP 800-171（3.1 アクセス制御ファミリー）に基づいており、以下の要件が含まれています。
#アクセス権の付与と取り消しに関するポリシーを実装する。
#許可された担当者のみにアクセスを制限してください。

#物理的資産およびデジタル資産を不正アクセスから保護します。
この質問は、情報、サービス、物理的な場所へのアクセスを許可または拒否するプロセスについて広く尋ねているため、正解はA. アクセス制御です。
* B. 物理的アクセス制御#不正解。物理的アクセス制御は、物理的な場所にのみ適用されるアクセス制御のサブセットです（例キーカード、警備員、生体認証）。この問題には情報とサービスも含まれるため、一般的なアクセス制御が正解です。
* C. 強制アクセス制御 (MAC)#不正解。MAC は、セキュリティ分類 (例: 極秘、秘密、機密) に基づいてアクセスが厳密に強制される特定のタイプのアクセス制御です。この問題では MAC が指定されていないため、これは不正解です。
* D. 裁量アクセス制御 (DAC)#不正解。DAC はアクセス制御の別の特定のタイプであり、データの所有者が誰がデータにアクセスできるかを決定します。この質問は一般的にアクセスを許可/拒否することについて尋ねているため、アクセス制御 (A) が最適な答えです。
他の回答が間違っている理由
* CMMC 2.0 モデル - AC.L2-3.1.1 ～ AC.L2-3.1.22 - 情報、サービス、物理空間へのアクセス制御を含むアクセス制御要件をカバーします。
* NIST SP 800-171 (3.1 - アクセス制御ファミリー) - アクセス制御の一般原則を定義します。
CMMC公式リファレンスによると、オプションA（アクセス制御）がCMMCアクセス制御要件に最も合致しているため、正解です。

最新問題: **160**
C3PAOが、評価を依頼したOSCのためにハイレベルスコープを実施しています。CMMCレベルの評価を依頼している契約に適用される人、プロセス、およびテクノロジーを表す用語はどれですか？
A. 支店
B. 調整ユニット
C. 支援組織／部署
D. ホストユニット
Answer: C (メーッセージを残す**)**

最新問題: **161**
評価チームによる評価中に、テストまたはデモンストレーションが実施されます。OSCは、どの環境でこのテストまたはデモンストレーションを実施しなければなりませんか？
A. クライアント
B. 開発
C. デモンストレーション
D. プロダクション
Answer: C (メーッセージを残す**)**

最新問題: **162**

主任評価者は、レベル2評価を完了するために必要なすべての作業が完了していることを確認します。最終的な評価結果パッケージは適切にレビューされ、アップロードの準備が整いました。主任評価者は、他にどのような資料の維持管理と保護を担当するのでしょうか？
A. 最終評価計画書、および主任評価者による評価プロセスの説明書簡
B. 評価に関するその他の注記および情報
C. C3PAOによる最終評価計画書および品質管理報告書
D. 最終評価計画書、主任評価者による結果説明書簡、およびC3PAOからの品質管理報告書
Answer: B (メーッセージを残す)

最新問題: **163**
主任評価者が参照し使用すべき主要な参考資料を最も適切に説明しているのは、次のうちどれですか？
A. レベル2評価のためのFAR条項52.204-21に基づく安全対策要件。
B. 希望する認証レベルに対応した、公開済みのCMMC評価ガイドの実践説明。
C. CMMCモデルの概要。評価方法と対象を提供します。
D. 国防総省が対象とする防衛情報に関する適切なセキュリティチェックリスト。
Answer: B (メーッセージを残す)

最新問題: **164**
評価チームのメンバーが、OSC（運用サービスセンター）に対してCMMCレベル2評価を実施しています。OSCは、AC.L1-3.1.1「情報システムへのアクセスを、承認されたユーザー、承認されたユーザーに代わって動作するプロセス、またはデバイス（他の情報システムを含む）に限定する」に基づいて評価対象を検査し、OSCから提供された証拠の妥当性を判断しています。この活動はどの評価方法に該当しますか？
A. テスト
B. 観察する
C. 検査する
D. インタビュー
Answer: C (メーッセージを残す)
CMMC 2.0における評価方法の理解CMMC評価プロセス（CAP）ガイドによると、評価者はセキュリティ対策への準拠を判断するために、主に3つの評価方法を使用します。
調査 - 文書、ポリシー、構成、およびシステム記録を確認する。
インタビュー :セキュリティプロセスに関する知見を得るために、担当者と面談する。
テスト :システム機能およびセキュリティ制御の技術的な検証を実施する。
評価チームのメンバーは、評価オブジェクト（システム構成、ユーザーアクセス制御設定、ポリシーなど）を検査し、OSC の証拠が AC.L1-3.1.1（アクセス制御 - 承認済みユーザー）に十分であるかどうかを判断します。
この活動は、以下のような成果物をレビューする「検査方法」に直接対応しています。

アクセス制御リスト（ACL）
システムユーザー認証ログ
アカウント管理ポリシー
役割ベースのアクセス制御設定
「観察する」（選択肢B）は、CMMCにおいて「観察」は公式の評価方法ではないため、誤りです。
「テスト」（選択肢A）は、評価が実際に機能を実行するのではなく、証拠を検証するものであるため、誤りです。
「インタビュー」（選択肢D）は、職員への質問は行われず、文書の確認のみが行われているため、誤りです。
CMMC評価プロセス（CAP）ガイド、第3.5項 - 評価方法
CMMCレベル2評価ガイド - アクセス制御の実践（AC.L1-3.1.1）
オプション C (検査) が正しい理由公式 CMMC ドキュメント参照最終検証このアクティビティは、アクセス制御措置を確認するためにドキュメントと記録をレビューすることを含むため、検査方法に該当し、オプション C が正解となります。

最新問題: **165**
RPOが提供するサービスの中で、最も包括的なサービスは何ですか？
A. トレーニングサービス
B. 教育サービス
C. コンサルティングサービス
D. アセスメントサービス
Answer: C (メーッセージを残す**)**
登録プロバイダー組織（RPO）の役割を理解する登録プロバイダー組織（RPO）は、CMMC認証を求める組織にコンサルティングサービスを提供するためにCMMC認定機関（CMMC-AB）によって認められた組織です。
RPOの主な機能#企業がCMMC評価に備えるためのコンサルティングサービス。
#コンプライアンスに必要なセキュリティ管理に関するガイダンス。
#文書作成、政策策定、ギャップ分析に関する支援。
#第三者によるCMMC評価の準備は行うが、公式のCMMC評価は実施しない（これはC3PAOの役割である）。
* コンサルティングサービスは、RPOの機能の中で最も広範かつ包括的なものです。
* RPOは評価を実施しない（選択肢Dは除外）。
* 研修や教育はコンサルティングの一部ではあるが、主要な機能ではない（AとBは除外される）。
コンサルティングには、研修、指導、文書作成支援、セキュリティ対策などが含まれており、最も包括的なサービスとなっています。
「コンサルティングサービス」が正解である理由は何ですか？回答選択肢の内訳オプションの説明正解ですか？

A：研修サービス
#誤り-RPO はトレーニングを提供する場合がありますが、これは彼らの主な機能ではありません。
B：教育サービス
#誤り - トレーニングに似ていますが、最も包括的なサービスではありません。
C :コンサルティングサービス
#正解 - RPOの中核機能はコンサルティングであり、これにはさまざまな準備サービスが含まれます。
D：評価サービス
#誤り - 公式のCMMC評価を実施できるのは、C3PAO（認定第三者評価機関のみです。
* CMMC-AB RPOプログラムでは、RPOを、企業がCMMC認証の準備をするのを支援するコンサルティング組織と定義していますが、評価は実施しません。
CMMC 2.0 ドキュメントからの公式参照最終検証と結論正解は C です。コンサルティング サービス RPO は主に CMMC 準拠の準備をしている組織に助言と準備サポートを提供します。

最新問題: **166**
CCP（認定認定専門家が、CMMCレベル2評価の評価チームメンバーとして活動しています。主任評価者は、OSC（運用支援センター）の構成管理（CM）ドメインの評価をCCPに割り当てました。CCPの最初のインタビュー相手は、ユーザーがインストールするソフトウェアの専門家です。ユーザーがインストールするソフトウェアに関して、CCPはインタビューでどの側面を重点的に取り上げるべきでしょうか？
A. 制御および監視
B. システムから削除されました
C. 悪意のあるコードをスキャンしました
D. 任務遂行に不可欠な用途のみに限定
Answer: A (メーッセージを残す**)**
CMMCレベル2における構成管理（CM）の理解CMMCレベル2では、構成管理（CM）ドメインは、不正な変更を防ぐためにシステムが安全に構成、保守、監視されることを保証する上で非常に重要です。CMの重要な側面の1つは、ユーザーがインストールしたソフトウェアの管理です。これは、適切に管理されないとセキュリティリスクを引き起こす可能性があります。
ユーザーがインストールしたソフトウェアを管理するための正しいアプローチは、NIST SP 800-171のCM.3.068に準拠しており、組織には以下のことが求められます。
#セキュリティを確保するために、構成設定を確立し、適用します。
組織のシステム上で、ユーザーがインストールしたソフトウェアを監視および制御し、不正なアプリケーションや安全でないアプリケーションが実行されないようにします。
制御および監視されている」が正しい理由とは？インタビューを実施するCCP（認定CMMCプロフェッショナル）は、ユーザーがインストールしたソフトウェアがCMMCレベ

ル2の要件に準拠するように制御および監視されているかどうかに焦点を当てる必要があります。これは、以下の点を確認することを意味します。
* ユーザーがインストールするソフトウェアの承認プロセス。
* ソフトウェアの変更を追跡するための監視メカニズム（システムログ、監査など）。
* セキュリティリスクを防止するため、不正なインストールを制限するポリシー。
回答選択肢の内訳
説明
正しい？
A：制御および監視されている
#CM.3.068への準拠を保証し、ユーザーがインストールしたソフトウェアが安全に管理されていることを確認します。
＃正しい
B: システムから削除されました
ソフトウェアは必ずしも削除する必要はありません。削除すべきなのは、不正なソフトウェアや危険なソフトウェアのみです。
＃正しくない
C: 悪意のあるコードをスキャンしました
スキャンは重要ですが（SI.3.218で説明）、構成管理の主要な焦点ではありません。
＃正しくない
D：任務遂行に不可欠な用途に限定
ソフトウェアの使用を制限することも有効だが、監視と制御こそが重要なセキュリティ対策である。
＃正しくない
* NIST SP 800-171、CM.3.068 - 「ユーザーがインストールしたソフトウェアの制御と監視」
* CMMC 2.0 レベル 2 の要件 - NIST SP 800-171 セキュリティ管理策に直接準拠しています。
CMMC 2.0 ドキュメントからの公式参照最終検証と結論正解は A です。
NIST SP 800-171のCM.3.068およびCMMC 2.0文書に従って、管理および監視されています。

有効な **CMMC-CCP** 問題集は GoShiken.com が提供された合格しやすい CMMC-CCP 試験問題集！ GoShiken.com が最新の **CMMC-CCP** 試験問題集を提供しています。GoShiken.com CMMC-CCP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CMMC-CCP 問題集をゲットする人はこちら: https://www.goshiken.com/Cyber-AB/CMMC-CCP-mondaishu.html (**23030%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題**: 167**
During an assessment, which phase of the process identifies conflicts of interest?
A. Analyze requirements.
B. Develop assessment plan.
C. Verify readiness to conduct assessment.
D. Generate final recommended assessment results.
Answer: (解答を表示する**)**
In the CMMC assessment process, conflicts of interest must be identified early to ensure an impartial and objective evaluation of an organization's compliance with CMMC 2.0 requirements. The appropriate phase for identifying conflicts of interest is during the"Verify Readiness to Conduct Assessment"phase.
Step-by-Step Explanation:
Assessment Planning & Conflict of Interest Consideration
Before an assessment begins, theC3PAO (Certified Third-Party Assessment Organization)or theDIBCAC (Defense Industrial Base Cybersecurity Assessment Center) for DOD-led assessmentsmust confirm that there are no conflicts of interest between assessors and the organization being assessed.
A conflict of interest may arise if an assessor haspreviously worked for, consulted with, or provided direct assistance tothe organization under review.
CMMC Assessment Process and Phases
The CMMC assessment process involves multiple steps, and the verification of readiness is acritical early phaseto ensure that the assessment is unbiased:
Analyze Requirements:This phase focuses on defining the assessment scope, but it does not include conflict of interest verification.
Develop Assessment Plan:This phase focuses on structuring the assessment methodology, not on identifying conflicts.
Verify Readiness to Conduct Assessment (Correct Answer):
At this stage, theC3PAO or assessment team must review potential conflicts of interest. TheDefense Industrial Base Cybersecurity Assessment Center (DIBCAC)also ensures assessors do not have any prior relationships that could compromise the objectivity of the evaluation.
Generate Final Recommended Assessment Results:This phase occurs at the end of the process, after the assessment is complete, so conflict of interest identification is too late by this stage.
Official CMMC Documentation & References
CMMC Assessment Process (CAP) Guide- The CAP details procedures assessors must follow, including conflict of interest verification.
CMMC 2.0 Scoping and Assessment Guides- Published by the Cyber AB and DoD, these guides reinforce the need for impartiality and independence in assessments.
DoD Instruction 5200.48 (Controlled Unclassified Information Program)- Outlines requirements for ensuring objective cybersecurity assessments.

評価実施準備状況の確認」段階で利益相反が特定されるようにすることで、CMMC認証プロセスの完全性が維持され、評価が公正かつ独立して、国防総省のサイバーセキュリティポリシーに従って実施されることが保証されます。

最新問題: **168**
CUI（機密情報）の取り扱いを必要とする契約を受注するために、請負業者は最低限どのレベルの認証を取得しなければならないか？
A. レベル2
B. レベル1
C. レベル3
D. どのレベルでも
Answer: B (メーッセージを残す**)**

最新問題: **169**
CMMCの上級レベルには、以下のアクセス制御（AC）の実践が含まれます。
A. レベル1
B. レベル3
C. レベル1とレベル2
D. レベル1、2、3
Answer: (解答を表示する**)**
CMMCモデルv2.0は累積型です。アドバンストレベル（レベル3）では、NIST SP 800-171（レベル2に準拠）の完全な実装が必要であり、NIST SP 800-172から追加のプラクティスのサブセットが追加されます。レベルは互いに積み重ねられていくため、レベル3のアクセス制御（AC）プラクティスには、必然的にレベル2のプラクティスが含まれます。
レベル1（基本的なFCI保護）、レベル2（CUI保護）、および追加のレベル3要件。
公式コンテンツからの補足抜粋：
CMMC モデル v2.0 の概要: 「このモデルは累積的であり、上位レベルのプラクティスには下位レベルのすべてのプラクティスが含まれます。」レベル 3 の説明: 「高度な...エキスパート レベルでは、NIST SP 800-171 に加えて NIST SP 800-172 のサブセットの実装が必要です。」オプション D が正しい理由:
上級レベルには、レベル1とレベル2のすべてのAC実践に加え、レベル3独自の追加実践が含まれます。
したがって、本書にはレベル1、レベル2、レベル3のアクセス制御手法が含まれています。
参考文献（CMMC v2.0公式コンテンツ）：
CMMCモデルv2.0、レベルの概要（実践の累積的な性質）。
NIST SP 800-171およびNIST SP 800-172（レベル2およびレベル3の制御源）。

最新問題: **170**
下請業者が有効なCMMC認証を取得していることを確認する責任は誰にありますか？

A. CMMC-AB
B. 米農務省
C. 国防総省機関またはクライアント
D. 請負業者組織
Answer: D (メーッセージを残す)
* 主契約者（契約組織）は、FCIまたはCUIを含む国防総省の契約に下請け業者を参加させる前に、下請け業者が必要なCMMC認証レベルを取得していることを確認する責任があります。
* この要件は、DFARS 252.204-7021 のフローダウン条項を通じて強制され、CUI を扱う下請業者は必要な CMMC レベル 2 またはレベル 3 の要件を満たすことが義務付けられています。
参照：
DFARS 252.204-7021（CMMC準拠）
CMMC 2.0 プログラムドキュメント
ステップ2：他の選択肢が間違っている理由A. CMMC-AB（不正解）：
Cyber AB（旧CMMC-AB）は、C3PAOの認定と評価プロセスの管理を担当していますが、下請け業者のコンプライアンスを強制する権限はありません。
B: OUSDA&S (誤り):
国防次官補（調達維持担当）室（OUSD A&S）はCMMCポリシーを策定・監督するが、個々の下請け業者の遵守状況を監視したり強制したりすることはない。
C：国防総省機関またはクライアント（誤り）：
While theDoD sets CMMC requirements, it relies onprime contractors to ensure compliance among their subcontractorsthrough contract flow-down requirements.
Final Confirmation of Correct Answer:Prime contractors must ensure their subcontractors have the required CMMC certification level to handle FCI or CUI.
Thus, the correct answer is:D. Contractor organization

最新問題**: 171**
ある従業員はOSCの主要システム管理者です。この従業員はシステムの管理と保守に関する業務のほとんどを担っているため、評価において中心的な役割を果たします。この従業員はどのような分類に最も適しているでしょうか？
A. アナライザー
B. 対象スタッフ
C. デモンストレーションスタッフ
D. 検査官
Answer: B (メーッセージを残す)

最新問題**: 172**

OSC（オープンサービスセンター）に対するレベル2評価が実施され、結果の提出準備が整いました。評価結果をアップロードする前に、C3PAO（認定3PAO）はどのような手順を完了する必要がありますか？
A. 結果の内部レビューを完了する。
B. CMMC-ABに提出予定であることを通知する。
C. 主任評価官とOSCの間で最終ブリーフィングを調整する。
D. 査定提出料をお支払いください。
Answer: (解答を表示する**)**

最新問題: **173**
評価担当者は、肯定的な意見を収集しています。これまでに、面接、実演、メール、メッセージ、プレゼンテーションなどを通じて情報を収集してきました。これらの方法は、肯定的な意見を収集する上で適切でしょうか？
A. いいえ、メールは適切な肯定の手段ではありません。
B. いいえ、メッセージを送ることは適切な肯定ではありません。
C. はい、査定員が収集した肯定的な回答はすべて適切です。
D. はい、査定担当者が収集した確認事項はすべて適切であり、スクリーンショットも同様です。
Answer: D (メーッセージを残す**)**
CMMC評価におけるアファメーションの理解アファメーションとは、CMMC評価中に収集される証拠の一種で、必須の実施事項への準拠を確認するためのものです。アファメーションは通常、以下の情報源から収集されます。
#インタビュー - セキュリティ対策を実施している担当者との会話。
#実演 - 実践の様子を観察する。
#メールとメッセージ - コンプライアンスへの取り組みを確認する書面によるコミュニケーション。
#プレゼンテーション - セキュリティ実装について説明する文書またはブリーフィング。
#スクリーンショット - システム構成とセキュリティ対策の視覚的な証拠。
* CMMC評価プロセス（CAP）ガイドでは、評価者は電子メール、メッセージ、プレゼンテーションなど、さまざまなコミュニケーション方法を通じて確認事項を収集できると規定されています。
* スクリーンショットは、コンプライアンスを確認するための有効な客観的証拠の追加形式です。
* オプションAとBは誤りです。なぜなら、メールやメッセージは、肯定の表明方法として明確に認められているからです。
* オプションCは、有効な証拠とみなされるスクリーンショットについて言及していないため、不完全です。
「はい、評価者が収集した肯定的な回答はすべて適切であり、スクリーンショットも同様です」が正しいのはなぜですか？

回答選択肢の内訳
説明
正しい？
A: いいえ、メールは適切な肯定の手段ではありません。
#メールアドレス欄に有効な確認方法がありません。
B :いいえ、メッセージを送ることは適切な肯定の表現ではありません。
#肯定的なメッセージを集めるために、不適切なメッセージも許可されています。
C :はい、査定担当者が収集した確認事項はすべて適切です。
#不正確なスクリーンショットも有効な証拠として考慮されるべきです。
D: はい、査定担当者が収集した確認事項はすべて適切であり、スクリーンショットも同様です。
#正解 - スクリーンショットも有効な証明方法です。
* CMMC評価プロセスガイド（CAP）- 書面によるコミュニケーションによる確認を含む、許容される証拠収集方法を定義します。
CMMC 2.0 ドキュメントからの公式参照最終検証と結論正解は D です。はい、評価者が収集した肯定文はすべて適切であり、スクリーンショットも同様です。これは、肯定文を収集するための CMMC 2.0 の評価手順と一致しています。

最新問題: **174**
CMMCレベル2評価の計画段階において、主任評価者は各実践事項について適切な証拠とは何かを検討します。評価者は何を検証しようとしているのでしょうか？
A. 適切性
B. 十分性
C. プロセスマッピング
D. 評価範囲
Answer: B (メーッセージを残す**)**
CMMCレベル2評価における証拠の十分性の理解CMMCレベル2評価では、主任評価者は、各実践について収集された証拠が評価結果を裏付けるのに十分であるかどうかを判断する必要があります。これは、評価者が以下を評価することを要求するCMMC評価プロセス（CAP）ガイドに準拠しています。
* 検査 - 文書、構成、およびシステム記録のレビュー。
* インタビュー - 担当者と話をして、実施状況と理解度を確認します。
* テスト - セキュリティ制御が実際に動作している様子を観察し、その有効性を検証する。
証拠が十分かどうかを判断するために、評価者は以下の点を確認します。
* 評価目標を直接的に支援する。
* その慣行が一貫して実施されていることを示す。
* 独自に検証可能です。
* 十分性とは、コンプライアンスについて正確な判断を下すのに十分な証拠が収集されているかどうかを指します。

* オプションA（適切性）は誤りです。適切性とは証拠の質に関することですが、十分性とは十分な証拠が存在するかどうかに関することです。
* オプションC（プロセス・マッピング）は、プロセス・マッピングはワークフローを理解するために使用されるものであり、評価検証方法ではないため、誤りです。
* オプションD（評価範囲）は誤りです。なぜなら、範囲の定義は証拠収集の前に、計画段階で行われるからです。
* CMMC評価プロセス（CAP）ガイド - セクション3.6（証拠の十分性の判断）
* CMMCレベル2評価ガイド - 証拠収集と評価
オプション B (十分性) が正しい理由公式 CMMC ドキュメント参照最終検証主任評価者がコンプライアンスを検証するのに十分な証拠が利用可能であることを確認しているため、正解はオプション B: 十分性です。

最新問題: **175**
実際の状況と期待される行動を比較する評価方法はどれですか？
A. テスト
B. 検査する
C. コンパイル
D. インタビュー
Answer: A (メーッセージを残す**)**
CMMC評価方法の理解
サイバーセキュリティ成熟度モデル認証（CMMC）2.0は、NIST SP 800-171Aの評価方法論に準拠しており、これには3つの主要な評価方法が含まれます。
調査する - ポリシー、手順、システム構成、およびドキュメントを確認する。
インタビュー：担当者と面談し、セキュリティ対策に関する理解度と実行状況を確認する。
テスト - セキュリティ制御が期待どおりに機能するかどうかを判断するために、実際の技術的または運用上のテストを実施する。
なぜ「テスト」が正解なのか？
「テスト」とは、実際に指定された条件と期待される動作を比較する方法のことです。
これは、システムが要求どおりに動作するかどうかを確認するために、手順、構成、または自動化ツールを実行することを含みます。
例えば、ポリシーで多要素認証（MFA）の適用が義務付けられている場合、テストではMFAなしでログインを試み、期待どおりにアクセスがブロックされるかどうかを確認する。
NIST SP 800-171Aガイド（CUIの評価手順）では、テストを次のような評価方法として定義しています。
セキュリティ制御が機能していることを積極的に検証する
現実世界の攻撃シナリオをシミュレートします
文書ではなくシステムアクションを通じてコンプライアンスをチェックする
他の回答が間違っている理由とは？
B) 検査する（不正解）

調査とは、ポリシー、手順、または構成を確認することのみを指し、システムの動作を積極的にテストするものではありません。
C). コンパイル（誤り）
「コンパイル」は、CMMC 2.0またはNIST SP 800-171Aにおける評価方法ではありません。
D) インタビュー（不正解）
インタビューは従業員から意見を収集するために用いられるが、実際の状況と期待される行動を比較するものではない。
結論
正解はAです。テストは、想定されるセキュリティ条件に対してシステムのパフォーマンスを積極的に検証するためです。
参考文献：
NIST SP 800-171A、「CUIのセキュリティ要件の評価」
CMMC 2.0評価プロセス（CAP）ガイド
国防総省CMMCスコープ設定および評価ガイドライン

最新問題: **176**
評価チームによる評価中に、テストまたはデモンストレーションが実施されます。OSCは、どの環境でこのテストまたはデモンストレーションを実施しなければなりませんか？
A. クライアント
B. 生産
C. 開発
D. デモンストレーション
Answer: B (メーッセージを残す**)**
* CMMCレベル2の評価では、評価者は、管理対象非機密情報（CUI）が取り扱われる実際の運用環境でセキュリティ管理が実施されていることを示す客観的な証拠を必要とします。
* これは、テストやデモンストレーションは、組織の実際のシステムとセキュリティ管理が使用されている本番環境で実施する必要があることを意味します。
* 評価チームは、セキュリティ対策が実際に適用される環境でその有効性を検証し、実際の運用条件下でセキュリティ対策が確実に機能していることを確認する必要があります。
* オプションA（クライアント）は、「クライアント」が定義された評価環境ではないため、誤りです。
* オプションC（開発）は、開発環境でのテストは本番環境のセキュリティ状況を正確に反映しないため、誤りです。
* オプション D (デモンストレーション) は誤りです。別のテスト環境でのデモンストレーションは CMMC 評価の有効な証拠とはならないため、実際のセキュリティ実装は運用環境で検証する必要があります。
* CMMC評価プロセス（CAP）ガイド - セクション3.5（評価方法）
* NIST SP 800-171 評価手順（検証は、CUI が存在する実際のシステムで行う必要があります。）評価環境要件の理解オプション B（本番環境が正しい理由公式 CMMC ドキュメント

参照最終検証CMMC 評価では、セキュリティ コントロールを実際の運用環境で検証する必要があるため、正解はオプション B：本番環境です。

最新問題: **177**
CMMCレベル2の評価方法には検査が含まれ、以下の項目が含まれる場合があります。
A. 文書、仕組み、または活動。
B. ポリシー、手順、セキュリティ計画、侵入テスト、およびセキュリティ要件。
C. システムバックアップ操作の監視、緊急時対応計画の実施、ネットワークトラフィックの監視。
D. システム内で採用されている特定のハードウェア、ソフトウェア、またはファームウェアの保護機能。
Answer: B (メーッセージを残す**)**

最新問題: **178**
各実践および／またはプロセスに必要な証拠は、以下の点に重点が置かれています。
A. 十分性と徹底性。
B. 適切性と十分性。
C. 適切性と徹底性。
D. 十分性と適切性。
Answer: B (メーッセージを残す**)**

最新問題: **179**
2人のネットワーク管理者が協力して、CMMCへの準拠に向けたネットワーク構成を決定しようとしています。しかし、いくつかの細かい点で意見が食い違うことが分かりました。CMMCへの準拠を確実にするための最適な解決策はどれでしょうか？
A. 会社のCEOに相談してください。
B. CMMC評価ガイドおよびNIST SP 800-171を参照してください。
C. 最も規制の緩いネットワーク管理者の意見に従う。
D. 最も厳格な制御を行うネットワーク管理者の考えに従う。
Answer: B (メーッセージを残す**)**
CMMC準拠の準備を行う際、組織はネットワーク構成が要求されるサイバーセキュリティ対策に準拠していることを確認する必要があります。ネットワーク管理者間で特定の構成について意見の相違が生じた場合、最も客観的かつ正確な解決方法は、CMMCレベル2の基礎となる公式のCMMCガイダンスおよびNIST SP 800-171の要件を参照することです。
* CMMC評価ガイドを主要な参考資料として使用する
* CMMC評価ガイド（レベル1およびレベル2）は、セキュリティ対策について明確な解釈を提供します。
* 各実践方法が認証プロセス中にどのように実施され、評価されるべきかを説明します。
* NIST SP 800-171を準拠基準とする

* CMMCレベル2は、機密指定されていない管理情報（CUI）を保護するために必要な110のセキュリティ管理策を概説したNIST SP 800-171に直接基づいています。
* ネットワーク構成は、NISTが定義するセキュリティ要件に準拠する必要があります。これには以下が含まれます。
* アクセス制御（AC）- 最小権限の原則を確保する。
* 監査および説明責任（AU）- ネットワーク活動のログ記録と監視。
* システムおよび通信保護 (SC) - 安全なネットワーク設計と暗号化。
* 他の選択肢が間違っている理由：
* (A) 会社のCEOに相談する：
* ACEOは必ずしもサイバーセキュリティの専門家ではなく、CMMCの技術要件に精通していない場合があります。
技術的なコンプライアンスに関する決定は、経営幹部の意見ではなく、CMMCおよびNISTのフレームワークに基づいて行うべきである。
* (C) ネットワーク管理者の提案に従い、最も緩やかな制御を行う。
* より緩やかな管理策を選択すると、セキュリティリスクが高まり、CMMCへの不準拠につながる可能性があります。
* (D) ネットワーク管理者の最も厳格な管理案に従う：
* セキュリティは重要ですが、より厳格な管理は、コンプライアンスのために必要ではない運用上の非効率性や不必要なコストをもたらす可能性があります。
正しいアプローチは、CMMCおよびNIST SP 800-171で要求されていることを実装することであり、それ以上でもそれ以下でもない。
* CMMC評価ガイドおよびNIST SP 800-171 Rev. 2は、コンプライアンスに関する最も信頼性の高いガイダンスを提供する公式の情報源です。
* CMMCレベル2はNIST SP 800-171に完全に準拠しており、セキュリティに関する意見の相違を解決するための決定的な情報源となっています。
手順ごとの詳細：CMMCドキュメントからの最終検証：したがって、正解は次のとおりです。
B：CMMC評価ガイドおよびNIST SP 800-171を参照してください。

最新問題: **180**
「情報の紛失、誤用、不正アクセス、または改ざんの結果と可能性に見合った保護措置」を表す用語はどれですか？
A. 十分なセキュリティ
B. 適応型セキュリティ
C. セキュリティ対策を採用
D. 高度なセキュリティ
Answer: A (メーッセージを残す**)**

最新問題: **181**

コンピュータおよび電子通信システム／サービス（それらに含まれる情報を含む）の損傷防止、保護、復旧を行い、その可用性、完全性、認証、機密性、否認防止を確保することを表す用語はどれですか？
A. ネットワークセキュリティ
B. 情報セキュリティ
C. データセキュリティ
D. サイバーセキュリティ
Answer: B (メーッセージを残す**)**

有効な **CMMC-CCP** 問題集は GoShiken.com が提供された合格しやすい CMMC-CCP 試験問題集！ GoShiken.com が最新の **CMMC-CCP** 試験問題集を提供しています。GoShiken.com CMMC-CCP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CMMC-CCP 問題集をゲットする人はこちら: https://www.goshiken.com/Cyber-AB/CMMC-CCP-mondaishu.html (**23030%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題**: 182**
レベル1の自己評価において、請負業者がFCIの基本的な安全対策要件を満たしていることを義務付けている規定または条項はどれですか？
A. FAR 52.204-21
B. 22CFR 120-130
C. DFARS 252.204-7011
D. DFARS 252.204-7021
Answer: (解答を表示する**)**
1. CMMCレベル1におけるFCIの基本的な保護要件の理解 連邦契約情報（FCI）は、政府によって契約に基づいて提供または生成された情報で、一般公開を意図していないものと定義されます。
CMMCレベル1は、FAR 52.204-21（対象となる請負業者の情報システムの基本的な保護）に記載されている15のセキュリティ要件に準拠し、FCIの基本的な保護を確保するように設計されています。
FCIのみを扱う請負業者は、FAR 52.204-21で定められた安全対策要件に直接準拠するCMMCレベル1を満たす必要があります。
2. FAR 52.204-21とCMMCレベル1準拠におけるその役割
FAR 52.204-21は、FCIを保護するために請負業者が実施しなければならない基本的なサイバーセキュリティ管理を定めています。
15の基本的な安全対策要件は以下のとおりです。
情報へのアクセスを許可されたユーザーのみに制限する。
システムへのアクセスを許可する前に、ユーザーを識別し認証する。

送信されたFCIを不正な開示から保護する。
外部システムへの接続を監視および制御する。
境界保護およびサイバーセキュリティ対策の適用。
廃棄前に培地を消毒する。
セキュリティ設定を更新して脆弱性を低減する。
物理的なセキュリティ対策を提供する。
FCIを処理するシステムへの物理的なアクセスを制御する。
該当する場合は、多要素認証（MFA）を強制的に適用する。
ソフトウェアおよびハードウェアの脆弱性を修正する。
リムーバブルメディアの使用を制限する。
システム監査ログの作成と保持。
リスクベースのセキュリティ評価を実施する。
インシデント対応計画の策定。
これら15のプラクティスは、CMMCレベル1自己評価の基礎を形成し、請負業者がFCIの取り扱いに関する最低限のサイバーセキュリティ要件を満たしていることを保証します。
3. 他の選択肢が間違っている理由
B) 22 CFR 120-130:
これは、防衛関連の物品およびサービスの輸出を規制する国際武器取引規則（ITAR）を指しており、FCIの安全保障要件とは関係ありません。
C). DFARS 252.204-7011:
この条項は代替的な明細項目構造に関するものであり、サイバーセキュリティやFCIの保護には関係しません。
D). DFARS 252.204-7021:
この条項は CMMC 要件を強制しますが、基本的な保護管理を定義しません。CMMC への準拠を要求しますが、基礎要件 (FAR 52.204- から得られる) を規定しません。
レベル1の場合は21）。
4. 公式CMMC 2.0リファレンスおよび学習ガイドとの整合性
CMMC 2.0 モデルのドキュメントでは、レベル 1 は FAR 52.204-21 の 15 の実践に重点を置いていることが確認されています。
国防総省の公式CMMCレベル1評価ガイドでは、FAR 52.204-21を満たすことがレベル1自己評価に合格するための要件であると明記されています。
CMMC 2.0 スコープガイドでは、FCI のみを取り扱い、レベル 1 認証を申請する請負業者は、FAR 52.204-21 のセキュリティ管理策のみを実施する必要があることが明確にされています。
最終確認：
正解はAです。FAR 52.204-21はFCIの基本的な保護を直接規定しており、CMMC 2.0のレベル1自己評価の基礎となる要件です。

最新問題: **183**

評価範囲を定める際、評価者は評価範囲が何を網羅しているかを確認すべきでしょうか？
A. 事業計画書に記載されているすべての資産
B. FCI/CUIを処理、保存、送信するかどうかにかかわらず、すべての資産
C. 事業分野を問わず、組織に関連するすべての事業体
D. FCI/CUIの処理、保管、送信を行うすべての資産、およびセキュリティ保護資産
Answer: D (メーッセージを残す**)**
CMMC評価におけるスコープ要件CMMC 2.0スコープガイドとCMMC評価プロセス（CAP）ドキュメントは、評価のスコープに含めるべき内容を明確に定義しています。
評価範囲には以下が含まれる必要があります。
* FCI/CUIを処理、保存、または送信するすべての資産
* セキュリティ保護資産（ESP）- これらの資産は、ファイアウォール、エンドポイント検出システム、暗号化メカニズムなど、FCI/CUIを保護するのに役立ちます。
したがって、正しい範囲には以下の両方が含まれます。
#FCI/CUI資産（データ保存、処理、または送信資産）
#セキュリティ保護資産（ESP）（ファイアウォール、セキュリティツールなど）
* A. 事業計画書に記載されているすべての資産#誤り。事業計画書にはFCI/CUIとは無関係の資産が含まれる場合があり、この範囲は広すぎます。FCI/CUIに関連する資産のみを評価する必要があります。
* B. FCI/CUI を処理、保存、または送信するかどうかにかかわらず、すべての資産#誤り。CMMC では、FCI/CUI と関連のない資産を含めることは組織に要求されていません。
* C. 事業分野に関係なく、組織に関連するすべての事業体#誤り。FCI/CUIまたはセキュリティ保護に関連する資産のみを評価する必要があります。無関係な事業部門（非連邦商業部門など）は対象外です。
他の回答が間違っている理由
* CMMC 2.0 スコープガイド - レベル1およびレベル2
* CMMC評価プロセス（CAP）文書
CMMC 公式リファレンスによると、公式の CMMC 評価範囲要件に従って、オプション D (FCI/CUI およびセキュリティ保護資産を処理、保存、または送信するすべての資産) が正解です。

最新問題**: 184**
評価手続きの最も一般的な目的は何ですか？
A. ハードウェアとソフトウェアの価値を決定する。
B. 証拠を入手する。
C. 情報フローを決定する。
D. 努力のレベルを定義する。
Answer: (解答を表示する**)**

最新問題**: 185**
各診療科における評価方法の最終決定権は誰にあるのですか？

A. 中国共産党
B. osc
C. サイトマネージャー
D. 主任評価者
Answer: (解答を表示する**)**
各診療科の評価方法は誰が決定するのか？
CMMCレベル2評価において、主任評価者は、各業務を評価するために使用される評価方法を決定する最終的な権限を有します。
主任評価者の主な責任
#CMMC評価プロセス（CAP）ガイドが遵守されていることを確認します。
面接、実演、文書レビューのいずれを使用して実務を評価するかを決定します。
#認定CMMCプロフェッショナル（CCP）およびその他の評価者に対し、証拠収集の方法論を指示する。
#適切な評価実施を保証するため、認定第三者評価機関（C3PAO）の下で業務を行います。
「主任評価者」という表現が正しい理由とは？
CCP（オプションA）は評価を支援するが、方法に関する最終決定は行わない。
OSC（オプションB）は認証を求める組織であり、評価方法を管理する組織ではありません。
サイトマネージャー（オプションC）は物流の調整を行うことはできますが、評価に関する決定権はありません。
回答選択肢の内訳
オプション
説明
正しい？
A). 中国共産党
#誤り - CCPassistsは評価方法を決定するものではありません。
B). OSC
#誤り - OSCは評価を受けている側であり、評価方法を決定する側ではありません。
C). サイトマネージャー
#誤り - サイトマネージャーは物流を担当しますが、評価方法を管理するわけではありません。
D) 主任評価者
#正解 - 主任評価者が使用する評価方法について最終決定権を持ちます。
CMMC 2.0ドキュメントからの公式参照
CMMC評価プロセスガイド（CAP）- 主任評価者の役割、すなわち評価方法の決定における役割を定義します。
最終検証と結論
正解はDです。主任評価者は、評価方法論に関する最終的な決定権を持っているからです。

最新問題: **186**

DoDI 5200.48: 管理対象非機密情報 (CUI) によると、CUI は誰によってマークされるのか？
A. 国防総省国防次官補
B. 正規の所有者
C. 情報公開担当者
D. 大統領が認可した原分類権限者
Answer: B (メーッセージを残す**)**
DoDI 5200.48では、CUIの認可保有者が適切なCUIマーキングを適用する責任を負うと規定されています。認可保有者とは、合法的な政府目的のために情報にアクセスできる個人を指します。これにより、情報の適切なマーキングに関する責任は、機密情報に適用される元の分類権限者だけでなく、資料を作成または取り扱う者にも及ぶことが保証されます。
参考資料：
* DoDI 5200.48、管理対象非機密情報（CUI）

最新問題**: 187**
クライアントが、CUI（機密情報）に該当すると合理的に判断されるデータを保存、処理、または送信するために、外部のクラウドベースサービスを利用しています。DFARS条項252.204-7012によれば、そのクラウドプロバイダーはどのような確立されたセキュリティ要件を満たさなければなりませんか？
A. FedRAMP Low
B. FedRAMP 中程度
C. FedRAMP High
D. FedRAMP Secure
Answer: B (メーッセージを残す**)**
DFARS 252.204-7012（保護対象防衛情報およびサイバーインシデント報告の保護）に基づき、請負業者がクラウドベースのサービスを使用して管理対象非機密情報（CUI）を保存、処理、または送信する場合、クラウドプロバイダーはFedRAMP Moderateまたは同等のセキュリティ要件を満たさなければなりません。
DFARS 252.204-7012 (c)(1) の主な要件:
クラウドに保存されるCUIは、FedRAMP Moderate（またはそれ以上）の要件に従って保護されなければなりません。
クラウドプロバイダーは、NIST SP 800-に準拠したFedRAMP Moderateベースラインセキュリティコントロールを満たす必要があります。
53 中程度のインパクトレベルの要件。
クラウドプロバイダーは、DFARS 252.204-7012に規定されているインシデント報告およびサイバーインシデント対応の要件への準拠も確保しなければなりません。
正解が「FedRAMP Moderate」（B）である理由は？
A). FedRAMP Low # 不正解
FedRAMP Lowは、機密性、完全性、可用性のリスクが低いシステムを対象としているため、CUI（機密情報）の保護には不十分です。

B). FedRAMP 中程度 # 正解
FedRAMP Moderateは、DFARS 252.204-7012に基づくCUIの最低必要レベルです。
これは、機密性は高いものの非機密扱いの政府データを保護するためのセキュリティ基準を提供するものです。
C). FedRAMP High # 不正解
FedRAMP Highは、機密性の高い情報（機密データや国家安全保障データなど）を扱うシステムに適用されますが、CUIには必ずしも必要ではありません。
D). FedRAMP Secure # 不正解
FedRAMPガイドラインには、公式なFedRAMP Secureカテゴリは存在しません。
CMMC 2.0 References Supporting this Answer:
DFARS 252.204-7012(c)(1)
Specifies thatcontractors using external cloud services for CUI must meet FedRAMP Moderate or equivalent.
CMMC 2.0 Level 2 Requirements
CUI must be protected using NIST SP 800-171 security requirements, whichalign with FedRAMP Moderate controls.
FedRAMP Security Baselines
FedRAMP Moderateis designed for systems that handlesensitive government data, including CUI.

最新問題**: 188**
主任評価担当者の自宅オフィスからほど近い顧客サイトで評価作業が行われています。顧客は作業期間中、ノートパソコンを提供しています。ネットワークエンジニアとのミーティング中、主任評価担当者はネットワークに関する情報を要求しました。エンジニアは、安全なクラウドストレージサービスを通じて提供できる図面が多数あると回答しました。主任評価担当者は自宅オフィスに戻り、これらの文書を確認することにしました。文書を取得する最善の方法は何でしょうか？
A. 評価者のラップトップからクライアントVPNにログインし、安全なクラウドストレージサービスからドキュメントを取得します。
B. クライアントのノートパソコンからクライアントVPNにログインし、安全なクラウドストレージサービスからドキュメントを取得します。
C. 安全なクラウドストレージサービスにログインして、ドキュメントのコピーを仕事用ノートパソコンとクライアント用ノートパソコンの両方に保存します。
D. 自宅のオフィスワークステーションを使用して、安全なクラウドストレージサービスからドキュメントを取得し、USB スティックに保存します。
Answer: B (メーッセージを残す**)**

Valid CMMC-CCP Dumps shared by GoShiken.com for Helping Passing CMMC-CCP Exam! GoShiken.com now offer the **newest CMMC-CCP exam dumps**, the GoShiken.com CMMC-CCP exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com CMMC-CCP dumps with Test Engine here: https://www.goshiken.com/Cyber-AB/CMMC-CCP-mondaishu.html (**230** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)