

EMC.D-CSF-SC-01.v2026-10-15.q79

試験コード:	D-CSF-SC-01
試験名称:	Dell NIST Cybersecurity Framework 2.0
認定資格:	EMC
無料問題数:	79
バージョン:	v2026-10-15
アクセス数:	126
ページビュー数:	790
https://www.jpnpdf.com/EMC.D-CSF-SC-01.v2026-10-15.q79-mondaishu.html	

最新問題: 1

サイバーセキュリティイベントを特定するという検出機能の目標をサポートするツールはどれですか？ (2つ選択してください)

- A. アイデンティティおよびアクセス管理 (IAM)
- B. 災害復旧計画 (DRP) ツール
- C. 侵入検知システム (IDS)
- D. セキュリティ情報およびイベント管理 (SIEM)

Answer: ([解答を表示する](#))

最新問題: 2

ある企業が侵入検知システムを導入したところ、非常に多くの誤報が発生していることに気づいた。

会社はこの状況を改善するためにどのような措置を講じるべきでしょうか？

- A. 侵入検知システムを侵入防御システムに置き換える
- B. ベースラインを再評価し、検出ルールに必要な調整を行う。
- C. 誤報を識別し、無視する方法を定義する
- D. 別のベンダーのシステムを評価することを検討する

Answer: ([解答を表示する](#))

最新問題: 3

NISTの識別機能において、資産目録を維持する主な目的は何ですか？

- A. 各資産のコストを決定する
- B. 資産を所有者別に分類する
- C. 資産を各部署に割り当てる
- D. サイバーセキュリティ保護が必要なリソースを特定し、優先順位付けする

Answer: D ([メッセージを残す](#))

最新問題: 4

重要インフラ分野全体に共通し、5つの同時かつ継続的な機能に合致する、サイバーセキュリティ活動、望ましい成果、および適用可能な参照事項の集合体とはどのようなものだろうか？

- A. プロフィール
- B. ガバナンス
- C. ベースライン
- D. コア

Answer: ([解答を表示する](#))

最新問題: 5

ビジネスインパクト分析 (BIA)の取り組みを支援するという識別機能の目標には、次のうちどれが含まれますか？ 2つ選択してください)

- A. 暗号化戦略
- B. 基本構成
- C. 資産の分類
- D. リスク評価プロセス

Answer: ([解答を表示する](#))

最新問題: 6

NISTサイバーセキュリティフレームワークのどのカテゴリが、組織内のコミュニケーションとデータフローのマッピングを保証するのでしょうか？

- A. ID.SC
- B. ID.RA
- C. ID.GV
- D. ID.AM

Answer: A ([メッセージを残す](#))

最新問題: 7

ある銀行が、照合システムの侵害について警告を受けました。この通知は、CEO宛てのメールで犯行声明を出したサイバー犯罪者から届きました。CEOは社内のCSIRTに警告を発しました。IRPのコミュニケーションプランでは、具体的にどのような事態を防ぐよう指示されていますか？

- A. キルチェーンの開始
- B. 性急な情報開示
- C. 保管管理記録の移転
- D. 回転率の向上

Answer: B ([メッセージを残す](#))

最新問題: 8

COBIT 2019ガバナンスシステムの主な目的は、____が全体的なビジネス戦略と整合していることを保証することです。

- A. IT運用
- B. サイバーセキュリティリスク
- C. 外部準拠基準
- D. ネットワーク稼働時間

Answer: B ([メッセージを残す](#))

最新問題: 9

大手オンライン小売業者の情報セキュリティマネージャーは、製品カタログデータベースが破損していると判断しました。同社は引き続きオンラインで注文を受け付けていますが、製品情報を更新できません。復旧にかかるダウンタイムは約4時間と見込まれています。製品カタログデータベースはどのような資産として分類されるべきでしょうか？

- A. ビジネス上極めて重要
- B. ミッションクリティカル
- C. 安全上極めて重要
- D. 非重要

Answer: A ([メッセージを残す](#))

最新問題: 10

COBIT 2019において、サイバーセキュリティフレームワークをカスタマイズするための重要な設計要素として考慮されるのは次のうちどれですか？

- A. 組織規模
- B. コンプライアンス規制
- C. 従業員の研修レベル
- D. 脅威インテリジェンスレポート

Answer: A ([メッセージを残す](#))

最新問題: 11

NISTサイバーセキュリティフレームワークを導入する際、導入プロセスにおける最初のステップは何ですか？

- A. 現在のサイバーセキュリティプロファイルを定義する
- B. コミュニケーションプランを作成する
- C. セキュリティポリシーのギャップを特定する
- D. リスク評価を実施する

Answer: A ([メッセージを残す](#))

最新問題: 12

COBIT 2019のどのコンポーネントが、NISTサイバーセキュリティフレームワークの「対応」機能に最も近いのか？

- A. サイバーセキュリティ予算編成
- B. インシデント対応
- C. リスク管理
- D. ITコンプライアンス

Answer: B ([メッセージを残す](#))

最新問題: 13

ランサムウェア攻撃を受けた後、組織のITチームはクラウドバックアップを使用してシステムの復旧とデータの回復を開始する。

この活動は、リカバリ機能のどのサブカテゴリに最もよく該当しますか？

- A. 継続的なモニタリング
- B. 異常検知
- C. コミュニケーション
- D. 復旧計画

Answer: D ([メッセージを残す](#))

最新問題: 14

各検出機能コンポーネントを、その主な目的と一致させてください。

成分

継続的なモニタリング

異常と事象

検出プロセス

脅威インテリジェンス

目的

- A) 不審な活動をリアルタイムで監視する
- B) 異常なパターンを特定する
- C) 検出プロトコルの形式化
- D) 脅威を特定するためのデータ分析

A. 継続的モニタリング - A

異常と事象 - C

検出プロセス - B

脅威インテリジェンス - D

B. 継続的モニタリング - D

異常と事象 - B

検出プロセス - C

脅威インテリジェンス - A

C. 継続的モニタリング - A

異常と事象 - B

検出プロセス - D

脅威インテリジェンス - C

D. 継続的モニタリング - A

異常と事象 - B

検出プロセス - C

脅威インテリジェンス - D

Answer: D ([メッセージを残す](#))

最新問題: 15

NISTサイバーセキュリティフレームワークのどの機能が、組織がサイバーセキュリティインシデントの影響を特定し、封じ込めることができるようにすることに重点を置いていますか？

A. 応答

B. 識別する

C. 検出

D. 回復

Answer: ([解答を表示する](#))

最新問題: 16

検出機能の文脈において、組織が異常な活動のパターンを特定するのに役立つ要素はどれですか？

A. データ暗号化

B. 脅威インテリジェンス

C. 資産運用

D. エンドポイント保護

Answer: B ([メッセージを残す](#))

有効な **D-CSF-SC-01** 問題集は GoShiken.com が提供された合格しやすい D-CSF-SC-01 試験問題集！ GoShiken.com が最新の **D-CSF-SC-01** 試験問題集を提供しています。GoShiken.com D-CSF-SC-01 試験問題は最新で、解答が正確でございます。最新の GoShiken.com D-CSF-SC-01 問題集をゲットする人はこちら：

<https://www.goshiken.com/EMC/D-CSF-SC-01-mondaishu.html> (**23230%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

職務分掌の目的は何ですか？

A. コラボレーションを促進する

B. 共謀を緩和し、窃盗を防止する

C. 不正行為を防止するための内部統制

D. 機能領域への露出を高める

Answer: ([解答を表示する](#))

最新問題: 18

NISTサイバーセキュリティフレームワークは、組織がサイバーセキュリティ体制を評価し、改善するのに役立つ___を使用します。

- A. プロフィール
- B. ベンダー評価
- C. ベンチマーク
- D. コンプライアンスチェック

Answer: A ([メッセージを残す](#))

最新問題: 19

対応機能のコンテキストにおいて、セキュリティインシデントを封じ込めるためにどのような措置が取られますか？

(2つ選択してください)

- A. 関係者への通知
- B. 影響を受けるシステムの隔離
- C. 根本原因分析の実施
- D. アクセス制御リストの更新

Answer: ([解答を表示する](#))

最新問題: 20

NISTサイバーセキュリティフレームワークにおける___プロファイルは、組織のリスク許容度と整合した、望ましいサイバーセキュリティの成果を表しています。

- A. 成熟
- B. 電流
- C. リスク
- D. ターゲット

Answer: D ([メッセージを残す](#))

最新問題: 21

ある小規模企業がNISTサイバーセキュリティフレームワークの導入を始めたばかりです。業務プロセスを見直し、データとインフラストラクチャを業務への影響度に応じて分類しています。この企業が最初に注力する可能性が高いフレームワーク機能は何でしょうか？

- A. 応答
- B. 識別する
- C. 保護
- D. 検出

Answer: B ([メッセージを残す](#))

最新問題: 22

医療機関は、患者データへのアクセスを許可された職員のみにより制限するために、厳格なアクセス制御を実施している。

この組織は、保護機能のどのサブカテゴリに重点を置いていますか？

- A. 基本構成
- B. データセキュリティ
- C. アクセス制御
- D. 保護技術

Answer: ([解答を表示する](#))

最新問題: 23

NISTサイバーセキュリティフレームワークにおける____機能は、組織に影響を与える可能性のある脆弱性や脅威を特定する責任を負っています。

- A. 検出
- B. 保護
- C. 識別する
- D. 回復

Answer: C ([メッセージを残す](#))

最新問題: 24

COBIT 2019フレームワークは、組織の戦略目標と整合するようにガバナンス構造を確立するためのガイダンスを提供します。

- A. サイバーセキュリティ対策
- B. 従業員研修プログラム
- C. 財務監査
- D. 操作手順

Answer: A ([メッセージを残す](#))

最新問題: 25

管理者は、4台のMicrosoft Windowsマシンがネットワークに参加したが、認証に必要な適切なレベルのパッチが適用されていないというアラートを受け取ります。

この問題に対応するカテゴリはどれですか？

- A. DE.DP
- B. DE.CM
- C. ID.AM
- D. DE.AE

Answer: B ([メッセージを残す](#))

最新問題: 26

組織の運営上の課題に対処するのに理想的な枠組みを提供する組織はどれでしょうか？

- A. NIST
- B. ISO
- C. COSO
- D. COBIT

Answer: B ([メッセージを残す](#))

最新問題: 27

サイバーセキュリティフレームワークを評価する際、COBIT 2019は、フレームワークを組織に合わせて調整するための重要な設計要素として___を強調しています。

- A. コンプライアンス義務
- B. 現在の技術インフラ
- C. 組織のリスク許容度
- D. 従業員向けサイバーセキュリティ研修

Answer: C ([メッセージを残す](#))

最新問題: 28

CSFは、IRPのコミュニケーションプランには、対象者、コミュニケーション方法、頻度、その他の要素を含めることを推奨しています。

- A. メッセージ基準
- B. インシデントの深刻度
- C. インシデントカテゴリ
- D. 使用するテンプレート

Answer: A ([メッセージを残す](#))

最新問題: 29

図を参照してください。貴社のセキュリティチームは、さまざまな事業部門と協力して、事業要件、リスク許容度、およびフレームワークプロファイルの作成に使用されるリソースを理解してきました。提供されたプロファイルに基づいて、ラベルA、B、およびCに対応するエントリはどれですか？

Action	Category	System	Risk Rank		Maturity		Priority	Cost
			SRC	TGT	SRC	TGT		
Detection Processes	A	ENG, FIN, Sales	3	8	4	6	7	4
		HR, EXEC	7	8	9	9	3	4
Security Continuous Monitoring	B	ENG, FIN, SALES, HR, EXEC	5	8	5	6	4	3
Anomalies and Events	C	ENG, FIN, SALES, HR, EXEC	6	8	5	7	6	6

A. A: PR.IP
B: DE.CM
C: DE.AE

B. A: PR.DS
B: DE.AE
C: DE.CM

C. A: DE.AE
B: PR.DS
C: RS.CO

A. オプションB
B. オプションA
C. オプションC

Answer: B ([メッセージを残す](#))

最新問題: 30

リカバリ機能で定義されている「通常の運用へのタイムリーな復旧」を確実にするために不可欠な要素は次のうちどれですか？

A. セキュリティアクセス制御
B. 継続的なモニタリング
C. 定期的なトレーニングセッション
D. 事業継続計画 (BCP)

Answer: D ([メッセージを残す](#))

最新問題: 31

組織が「現状」と「将来像」の文書を比較し、サイバーセキュリティ体制を改善する機会を特定するのに役立つものは何でしょうか？これは、組織の現状の基準と将来目指すべき状態を把握し、ギャップ分析を実施するために役立ちます。

A. 評価
B. コア
C. プロフィール
D. フレームワーク

Answer: C ([メッセージを残す](#))

有効な **D-CSF-SC-01** 問題集は GoShiken.com が提供された合格しやすい D-CSF-SC-01 試験問題集！ GoShiken.com が最新の **D-CSF-SC-01** 試験問題集を提供しています。GoShiken.com D-CSF-SC-01 試験問題は最新で、解答が正確でございます。最新の GoShiken.com D-CSF-SC-01 問題集をゲットする人はこちら：

最新問題: 32

COBIT 2019フレームワークにおけるガバナンスの目的は、___が組織全体で一貫して対処されるようにすることです。

- A. リスク管理
- B. 継続的な改善
- C. データプライバシー
- D. セキュリティポリシーの更新

Answer: A ([メッセージを残す](#))

最新問題: 33

レスポンス関数を構成する5つのカテゴリは何ですか？

- A. 対応計画、コミュニケーション、分析、緩和、および改善
- B. 対応計画、データセキュリティ、コミュニケーション、分析、および緩和
- C. 緩和、改善、維持、対応計画、ガバナンス
- D. 意識向上と研修、改善、コミュニケーション、分析、ガバナンス

Answer: A ([メッセージを残す](#))

最新問題: 34

識別機能内の制御に基づいて開発できるKPIはどれですか？ 2つ選択してください)

- A. 在庫監査の頻度
- B. 分類が更新された資産の割合
- C. 年間報告件数
- D. サイバーセキュリティ意識向上トレーニングを受けたユーザー数

Answer: A,B ([メッセージを残す](#))

最新問題: 35

組織のシステムにおけるセキュリティ状況に関する状況認識を高める活動とはどのようなものか？

- A. DPI
- B. ISCM
- C. IDP
- D. RMF

Answer: B ([メッセージを残す](#))

最新問題: 36

NISTサイバーセキュリティフレームワークは、主にどのような要素に基づいて構成されていますか？ 2つ選択してください)

- A. ロードマップ
- B. 目的
- C. ティア
- D. コア

Answer: C,D ([メッセージを残す](#))

最新問題: 37

サイバーセキュリティフレームワークにおける主要なカテゴリの1つは___であり、これは重要なインフラサービスの保護に重点を置いています。

- A. 意識向上トレーニング
- B. 保護技術
- C. リスク評価
- D. 資産運用

Answer: B ([メッセージを残す](#))

最新問題: 38

情報セキュリティ継続監視においてデータ収集を行う際に考慮すべき事項は何ですか？

- A. 自動化によりデータ収集効率が向上します。
- B. データはネットワークを通過する際に最もよく取得されます。
- C. 収集はコンプライアンス要件のみに使用されます。
- D. 収集するデータが多いほど、異常を検知できる可能性が高くなります。

Answer: ([解答を表示する](#))

最新問題: 39

ベースライン評価の目的は何ですか？

- A. コストを決定する
- B. リスクを判断する
- C. 展開時間を短縮する
- D. データ整合性の向上

Answer: ([解答を表示する](#))

最新問題: 40

NISTサイバーセキュリティフレームワークのどのティアが、進化する脅威に基づいてサイバーセキュリティ対策を適応させる組織を表していますか？

- A. ティア4：適応型
- B. ティア2：リスク情報に基づく
- C. ティア3：繰り返し可能
- D. ティア1：部分的

Answer: ([解答を表示する](#))

最新問題: 41

最高情報セキュリティ責任者 (CISO) は、コスト削減、全体的な効率向上、およびセキュリティ関連情報の監視の信頼性向上を実現するソリューションを求めている。

どのISCM機能が推奨されますか？

- A. 自動化
- B. コレクション
- C. プロビジョニング
- D. 報道

Answer: A ([メッセージを残す](#))

最新問題: 42

リカバリ機能の主な目的は何ですか？

- A. ワークロード、アセット、監査ログを復元する
- B. バックアップの復元、脅威の分析、バックアップの整合性の監視
- C. 資産、ワークロード、およびサービスを復元する
- D. サービスの復旧、リスクの軽減、改善

Answer: ([解答を表示する](#)**)**

最新問題: 43

識別機能内で、ビジネス影響分析は、サイバーセキュリティインシデントが発生した場合に_____を判断するのに役立ちます。

- A. 人事方針
- B. 資産減価償却率
- C. 重要なビジネス機能
- D. 予算配分

Answer: C ([メッセージを残す](#))

最新問題: 44

リスク管理戦略に関して、経営幹部はどのような情報伝達に責任を負うべきでしょうか？

- A. リスク軽減
- B. 資産リスク
- C. リスクプロファイル
- D. リスク許容度

Answer: ([解答を表示する](#)**)**

最新問題: 45

NISTサイバーセキュリティフレームワークの主な構成要素は何ですか？

- A. コア、ティア、プロファイル
- B. 機能、プロファイル、および階層
- C. カテゴリ、階層、プロフィール

D. コア、カテゴリー、ティア

Answer: A ([メッセージを残す](#))

最新問題: 46

企業は、現在のサイバーセキュリティ活動を把握し、業界標準に準拠させるために、全体像を把握する必要があります。また、将来の改善に向けたロードマップも求めています。彼らはNISTフレームワークのどの構成要素に注力すべきでしょうか？

A. コア

B. 目的

C. プロフィール

D. ティア

Answer: ([解答を表示する](#))

有効な **D-CSF-SC-01** 問題集は GoShiken.com が提供された合格しやすい D-CSF-SC-01 試験問題集！ GoShiken.com が最新の **D-CSF-SC-01** 試験問題集を提供しています。GoShiken.com D-CSF-SC-01 試験問題は最新で、解答が正確でございます。最新の GoShiken.com D-CSF-SC-01 問題集をゲットする人はこちら：

<https://www.goshiken.com/EMC/D-CSF-SC-01-mondaishu.html> (**23230%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

貴社はサイバー攻撃を受けました。貴社はCSIRT（コンピュータセキュリティインシデント対応チーム）に報告し、CSIRTは攻撃を封じ込め、脅威を排除しました。将来的に効果的なCSRL（顧客関係責任報告書とより強固なサイバーセキュリティ体制を確保するために、次に必要なステップは何でしょうか？

A. 変化の担い手を特定する

B. ギャップ分析を実施する

C. BIAを更新する

D. BCPを更新する

Answer: C ([メッセージを残す](#))

最新問題: 48

ある小売企業が顧客記録に影響を与えるデータ侵害に見舞われた。インシデント対応計画では、即時の封じ込めと影響を受けた顧客への連絡が求められている。この対応において、対応機能のどのサブカテゴリが直接的に扱われているか？

A. リスク評価とトレーニング

B. 封じ込めと通信

C. 検出と分析

D. 復旧と文書化

Answer: B ([メッセージを残す](#))

最新問題: 49

回収不能資産は、具体的にどの機能で扱われますか？

A. 保護

B. 回復

C. 識別する

D. 応答

Answer: C ([メッセージを残す](#))

最新問題: 50

NISTサイバーセキュリティフレームワークにおける____機能は、サービスを保護するための適切な安全対策を開発および実装する責任を負います。

A. 回復

B. 識別する

C. 検出

D. 保護

Answer: D ([メッセージを残す](#))

最新問題: 51

どのカテゴリが、ソフトウェアにおける不正コードの検出に対応していますか？

A. PR.AT

B. DE.CM

C. PR.DS

D. DE.DP

Answer: B ([メッセージを残す](#))

最新問題: 52

USBデバイスへのアクセスを制限し、社内での使用を防止するために使用される技術的な制御は、何によって決定されるのでしょうか？

A. 全従業員によるUSB機器の使用を禁止する

B. USBデバイスの使用を禁止するセキュリティポリシー

C. 従業員向け人事研修における利用規約

D. USBデバイスの使用を検出し、使用者を報告する

Answer: A ([メッセージを残す](#))

最新問題: 53

_____の目的は、インシデント後の対応措置の有効性を評価し、改善すべき領域を特定することです。

- A. インシデント記録
- B. 対応計画
- C. 事後検証
- D. インシデント検出

Answer: C ([メッセージを残す](#))

最新問題: 54

ある企業が、フィッシング攻撃を認識するための意識向上研修を全従業員を対象に実施している。

この活動は、保護機能のどの部分に該当しますか？

- A. データセキュリティ
- B. アクセス制御
- C. 意識向上とトレーニング
- D. 保護技術

Answer: C ([メッセージを残す](#))

最新問題: 55

どのような種類のシステムが情報処理を行っており、そのシステムが失われると組織に深刻な影響を与える可能性があるか？

- A. ミッションクリティカル
- B. 安全上極めて重要
- C. ビジネス上極めて重要
- D. セキュリティ上極めて重要

Answer: A ([メッセージを残す](#))

最新問題: 56

NISTサイバーセキュリティフレームワークの___機能は、サイバーセキュリティインシデントの影響を軽減することを目的としています。

- A. 保護
- B. 検出
- C. 回復
- D. 応答

Answer: D ([メッセージを残す](#))

最新問題: 57

CMDBには何を含める必要がありますか？

- A. アンインストールされたソフトウェアのインベントリ
- B. ソフトウェアエンドユーザーライセンス契約
- C. インストール済みコンポーネントの依存関係
- D. インストールされているソフトウェアの既知の脆弱性

Answer: C ([メッセージを残す](#))

最新問題: 58

ある組織のセキュリティチームは、セキュリティ情報およびイベント管理 (SIEM) システムからのログを分析し、異常なパターンを特定しようとしている。

このアクティビティは、検出機能のどのサブカテゴリをサポートしていますか？

- A. 検出プロセス
- B. セキュリティ意識
- C. 継続的なモニタリング
- D. 異常と事象

Answer: ([解答を表示する](#))

最新問題: 59

NISTサイバーセキュリティフレームワークの保護機能に通常含まれない活動はどれですか？

- A. 継続的なモニタリング
- B. インシデント対応計画
- C. データセキュリティポリシー
- D. アクセス制御管理

Answer: A ([メッセージを残す](#))

最新問題: 60

識別機能におけるギャップ分析の主な目的は何ですか？

- A. その機能に関連するサイバーセキュリティフレームワークとサイバーレジリエントライフサイクルの間のギャップを特定する
- B. 現在のプロファイル状態から目標プロファイル状態へ移行するために必要なアクションを決定する
- C. セキュリティ対策を強化するためのセキュリティ管理策を決定する。
- D. 業務プロセスのギャップを特定し、業務効率を向上させる

Answer: B ([メッセージを残す](#))

最新問題: 61

継続的に更新されるCMDBは、NISTのどの機能およびカテゴリの出力ですか？

- A. ID.BE
- B. ID.AM
- C. ID.RM
- D. ID.SC

Answer: B ([メッセージを残す](#))

有効な **D-CSF-SC-01** 問題集は GoShiken.com が提供された合格しやすい D-CSF-SC-01 試験問題集！ GoShiken.com が最新の **D-CSF-SC-01** 試験問題集を提供しています。GoShiken.com D-CSF-SC-01 試験問題は最新で、解答が正確でございます。最新の GoShiken.com D-CSF-SC-01 問題集をゲットする人はこちら：

<https://www.goshiken.com/EMC/D-CSF-SC-01-mondaishu.html> (232**30%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

どの文書に、キャッシュフローの損失、設備交換費用、受注残に対する給与、および不具合に関連する財務損失が記載されていますか？

- A. リスク評価戦略
- B. 災害復旧計画
- C. 事業影響分析
- D. 事業継続計画

Answer: ([解答を表示する](#))

最新問題: 63

COBIT 2019に準拠したサイバーセキュリティフレームワークの実装を開始する際に、最も重要な最初のステップは次のうちどれですか？

- A. ステークホルダー向けコミュニケーションプランの作成
- B. ガバナンス構造の現状把握
- C. コンプライアンス要件の決定
- D. 既存のサイバーセキュリティ機能の特定

Answer: D ([メッセージを残す](#))

最新問題: 64

医療機関のインシデント対応計画には、セキュリティ侵害発生後72時間以内に関係規制機関に通知する手順が含まれている。

この活動は、応答機能のどのサブカテゴリを満たしていますか？

- A. コミュニケーションプラン
- B. 回復戦略
- C. 検出と分析
- D. 事後検証

Answer: ([解答を表示する](#))

最新問題: 65

組織が業務、資産、および個人に対するセキュリティリスクを確実に理解するために、どのような方法が用いられますか？

- A. リスクプロファイル

- B. 運用評価
- C. リスク評価
- D. リスク管理戦略

Answer: C ([メッセージを残す](#))

最新問題: 66

組織にとって損害を最小限に抑え、復旧時間を短縮し、可能な限りコストを削減するために設計された文書はどれですか？

- A. 事業継続計画
- B. 事業影響分析
- C. インシデント対応計画
- D. リスク評価戦略

Answer: A ([メッセージを残す](#))

最新問題: 67

NISTサイバーセキュリティフレームワークは、COBIT 2019をどのように補完するのでしょうか？

- A. 技術導入ガイドを提供することにより
- B. ITプロセスをビジネス目標に合わせることで
- C. ガバナンスとコンプライアンスに重点を置くことで
- D. 詳細な技術制御を提供することにより

Answer: C ([メッセージを残す](#))

最新問題: 68

NISTサイバーセキュリティフレームワークの構造は、いくつかのコア機能を中心に構築されていますか？

- A. 6
- B. 4
- C. 7
- D. 5

Answer: ([解答を表示する](#))

最新問題: 69

BIAの範囲外とみなされるものは何ですか？

- A. バックアップに必要な容量要件の決定
- B. 既存のリスク軽減策の効率性と有効性
- C. フルバックアップ、増分バックアップ、差分バックアップの選択
- D. 特定された脅威が実際に発生する推定確率

Answer: ([解答を表示する](#))

最新問題: 70

サイバーセキュリティフレームワークの中核は、いくつかのカテゴリで構成されていますか？

- A. 16
- B. 28
- C. 23
- D. 10

Answer: C ([メッセージを残す](#))

最新問題: 71

NISTサイバーセキュリティフレームワークにおける「識別」セクションの主な機能は何ですか？

- A. 組織の状況とリスク許容度を理解する
- B. 資産へのアクセス管理
- C. サイバーセキュリティインシデントからの復旧
- D. サイバーインシデントの検知と対応

Answer: ([解答を表示する](#)**)**

最新問題: 72

NISTサイバーセキュリティフレームワークにおいて、サイバーセキュリティインシデント発生後も重要な機能の継続性を確保する上で、以下のどの要素が鍵となりますか？

- A. 識別する
- B. 回復
- C. 検出
- D. 保護

Answer: ([解答を表示する](#)**)**

最新問題: 73

組織がセキュリティ体制をリアルタイムで管理するためのリスク管理上の意思決定を行う上で、どのような支援が必要となるのでしょうか？

- A. ユーザーアクセスレビュー
- B. ベースライン報告
- C. ビデオ監視
- D. 継続的なモニタリング

Answer: D ([メッセージを残す](#))

最新問題: 74

資産管理ソフトウェアアプリケーションを使用して、組織内でどのようなものを在庫として管理すべきでしょうか？

- A. データ、デバイス、ソフトウェア、監査ログ

- B. データ、ペルソナ、アイデンティティ、CMDB
- C. データ、プロフィール、ソフトウェア、およびシステムログ
- D. データ、デバイス、ID、ソフトウェア

Answer: ([解答を表示する](#))

最新問題: 75

検出機能内で継続的な監視を実装することによるメリットは次のうちどれですか？ 2つ選択してください

- A. ネットワーク活動の可視性の向上
- B. アクセス制御管理の改善
- C. セキュリティインシデントの早期発見
- D. ハードウェアコストの削減

Answer: ([解答を表示する](#))

最新問題: 76

COBIT 2019のサイバーセキュリティリスクへの重点は、NISTサイバーセキュリティフレームワークのどの構成要素と一致しますか？

- A. 応答
- B. ガバナンス
- C. ティア
- D. プロフィール

Answer: B ([メッセージを残す](#))

有効な **D-CSF-SC-01** 問題集は GoShiken.com が提供された合格しやすい D-CSF-SC-01 試験問題集！ GoShiken.com が最新の **D-CSF-SC-01** 試験問題集を提供しています。GoShiken.com D-CSF-SC-01 試験問題は最新で、解答が正確でございます。最新の GoShiken.com D-CSF-SC-01 問題集をゲットする人はこちら：

<https://www.goshiken.com/EMC/D-CSF-SC-01-mondaishu.html> (**23230%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

ある組織が、独自のリスクプロフィールとビジネス要件に合わせて、NISTサイバーセキュリティフレームワークのカスタマイズ版を作成している。現在、組織の優先事項とリスク許容度をフレームワークの機能にマッピングしているところだ。

彼らはNISTフレームワークのどの部分に焦点を当てているのでしょうか？

- A. プロフィール
- B. コア
- C. 目的

D. ティア

Answer: A ([メッセージを残す](#))

最新問題: 78

組織がデジタル資産を保護する際に実施する一般的なプロセスの中で、NISTサイバーセキュリティフレームワークの適用範囲外となるものはどれですか？

- A. 調査する
- B. 識別する
- C. 保護
- D. 回復

Answer: A ([メッセージを残す](#))

最新問題: 79

NISTサイバーセキュリティフレームワークにおける___機能は、主にサイバーセキュリティインシデント発生後の回復力維持に重点を置いています。

- A. 回復
- B. 保護
- C. 識別する
- D. 応答

Answer: ([解答を表示する](#))

Valid D-CSF-SC-01 Dumps shared by GoShiken.com for Helping Passing D-CSF-SC-01 Exam! GoShiken.com now offer the **newest D-CSF-SC-01 exam dumps**, the GoShiken.com D-CSF-SC-01 exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com D-CSF-SC-01 dumps with Test Engine here: <https://www.goshiken.com/EMC/D-CSF-SC-01-mondaishu.html> (232 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)