ISC.CISSP.v2022-11-28.q522

試験コード:	CISSP
試験名称:	Certified Information Systems Security Professional (CISSP)
認定資格:	ISC
無料問題数:	522
バージョン:	v2022-11-28
アクセス数:	5578
ページビュー数:	5210
https://www.jpnpdf.com/ISC.CISSP.v2022-11-28.q522-mondaishu.html	

最新問題: **1**
次の一般的なデータネットワークサービスのどれが電子メールの送受信に使用されますか
電子メールゲートウェイデバイスを介して内部または外部？
A. ファイルサービス
B. メールサービス
C. 印刷サービス
D. クライアント/サーバーサービス
Answer: B (メーッセージを残す)
この機能はメールサービスを通じて提供されます。このサービスにより、内部レベルと外部レベルのユーザー間のコラボレーションが可能になります。通常、2つのプロトコルを使用します。ポートTCP 25の「SMTP」で電子メールを送信し、ポートTCP110の「POP3」で電子メールを受信します。現在人気を集めている別のプロトコルがあります、それは「IMAP4」です。印刷サービスはドキュメントの印刷に使用され、ファイルサービスはインフラストラクチャ内のファイルとフォルダーの共有とアクセスに使用されます。

最新問題: **2**
次のうち、システムの通常のセキュリティメカニズムによって保護されていない意図しない通信パスはどれですか？
A. 信頼できるパス
B. 保護ドメイン
C. 被覆通信路
D. メンテナンスフック
Answer: C (メーッセージを残す)
秘密チャネルは、システム内の意図しない通信パスであるため、
システムの通常のセキュリティメカニズムによって保護されていません。隠密チャネルは秘密の方法です

情報を伝える。
秘密チャネルは、TCSECレベルB2からアドレス指定されます。
以下は不正解です。
トラステッドパスは、ユーザーがトラステッドコンピューティングベースにアクセスできるようにする保護されたチャネルです。
（TCB）他のプロセスやユーザーに妥協されることなく。
保護ドメインは、各プロセスに割り当てられた実行スペースとメモリスペースで構成されます。
メンテナンスフックは、システムを許可するためにインストールされたハードウェアまたはソフトウェアのメカニズムです。
メンテナンスとシステムのセキュリティ保護をバイパスします。
この質問に使用される参照：
KRUTZ、Ronald L.＆VINES、Russel D.、CISSP準備ガイド：の10のドメインをマスターする Computer Security、John Wiley＆Sons、2001年、第6章：運用セキュリティ（219ページ）。

最新問題: 3
次の回答のうち、ネットワークベースのIDSまたはIPSシステムに最も重大な脅威をもたらすものはどれですか？
A. 暗号化されたトラフィック
B. 複雑なIDS/IPS署名構文
C. デジタル署名されたネットワークパケット
D. 分離されたVLAN
Answer: (解答を表示する**)**
考察：暗号化されたネットワークパケットは、ネットワークを簡単に（または迅速に）デコードおよび検査できないため、効果的なIDS/IPS計画に最大の脅威をもたらします。
IDSは暗号化されたパケットを調べて脅威があるかどうかを判断できないため、ほとんどの場合、トラフィックは潜在的な脅威とともに転送されるだけです。
企業がネットワークトラフィックの検査サービスを提供し、すべてのネットワークトラフィックのプロキシサーバーのように機能する業界があります。
証明書のコピーを送信するだけで、トラフィックをデコードできます。これは、連邦法に違反したり、インサイダー取引のために連邦捜査官に訴えられたりすると、ビジネスが崩壊する可能性がある金融業界では一般的です。
外部の会社は、潜在的な責任について、ネットワークとの間で送受信されるすべてのネットワークトラフィックを調べます。
次の答えは正しくありません。
-複雑なIDS/IPS署名構文：IDS / IPS署名は複雑になる可能性がありますが、これはIDS/IPSシステムの機能に対する最も重大な脅威ではありません。
-デジタル署名されたネットワークパケット：危険なネットワークトラフィックを探しているIDS / IPSシステムにとって脅威ではないため、これは不正解です。何よりも、送信する各ネットワークパケットにデジタル署名することは一般的ではないためです。

-分離されたVLAN :これは正解ではありませんが、VLANは、危険なトラフィックを検出するIDS/IPSシステムに対する障壁となる可能性があります。VLANとIDS/IPSシステムには簡単な解決策があり、そのVLANにIDS / IPSセンサーを配置し、そのVLANをIDS/IPS管理システムに送信するように設定するだけです。
この質問を作成するために、次の参照が使用されました。
グレッグ、マイケル; ヘインズ、ビリー（2012-02-16）。CASP :CompTIA Advanced Security Practitioner
学習ガイド認定コースウェア：試験CAS-001（Pg。138）Wiley。キンドル版。

最新問題**: 4**
バックアップされたファイルのアーカイブビットをリセットしないバックアップ方法はどれですか？
A. 完全バックアップ方式
B. 増分バックアップ方式
C. 差分バックアップ方式
D. 追加バックアップ方式
Answer: C (メーッセージを残す**)**
差分バックアップ方式では、最後の完全バックアップが実行されてから変更されたファイルのみがコピーされます。アーカイブビットをリセットしないため、変更または追加されたすべてのファイルは、次の完全バックアップまですべての差分バックアップでバックアップされるという点で付加的です。 「追加バックアップ方式」は、一般的なバックアップ方式ではありません。出典：KRUTZ、Ronald L.＆VINES、Russel D.、CISSP Prep Guide :Mastering the Te n Domains of Computer Security、John Wiley＆Sons、2001、Chapter 3 :Telecommunications and Network Security（69ページ）。

最新問題**: 5**
Kerberosの弱点のいくつかに対処するために開発され、秘密鍵の配布に公開鍵暗号化を使用し、追加のアクセス制御サポートを提供するのは、次のうちどれですか？
A. ゴマ
B. RADIUS
C. KryptoKnight
D. TACACS +
Answer: A (メーッセージを残す**)**
説明/参照：
Explanation:
マルチベンダー環境でのアプリケーション向けの安全なヨーロッパシステム（$ESAME）は、Kerberosの弱点のいくつかに対処するために開発され、秘密鍵の配布に公開鍵暗号を使用し、追加のアクセス制御サポートを提供します。
不正解：

B :RADIUSは、クライアント/サーバーの認証と承認を可能にし、リモートユーザーを監査するネットワークプロトコルです。Kerberosの弱点のいくつかに対処するために開発されたわけではありません。
C :KryptoKnightは、ネットワーク環境内のアプリケーションと通信エンティティに認証と鍵配布サービスを提供します。Kerberosの弱点のいくつかに対処するために開発されたわけではありません。
D :TACACS +は、クライアント/サーバーの認証と承認を可能にするネットワークプロトコルです。Kerberosの弱点のいくつかに対処するために開発されたわけではありません。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、2013、pp.214、234-236
http://www.eurecom.fr/~nsteam/Papers/kryptoknight.pdf

最新問題**: 6**
ソフトウェア開発プロセスのスパイラルモデル（BW Boehm、A
ソフトウェア開発と拡張のスパイラルモデル、IEEE
Computer、May、1988）は、スパイラルに関連して次のメトリックを使用します。
A. 角度寸法は累積コストを表します
B. 半径寸法は累積コストを表します
C. 半径方向の寸法は、それぞれの完了の進捗状況を表します
サイクル
D. 半径寸法は各フェーズのコストを表します
Answer: B (メーッセージを残す**)**
半径寸法は累積コストと角度を表します
ディメンションは、の各サイクルを完了する際の進捗状況を表します
螺旋。スパイラルモデルは、実際にはソフトウェア開発プロセスのメタモデルです。スパイラルのステージの概要は次のとおりです。
スパイラルは、上部の左側の象限で開始されます。
開発中の製品の部分の目的、
製品のこの部分を実装するための代替手段、および
代替案の適用に課せられた制約。
次に、代替案のリスクは、以下に基づいて評価されます。
目的と制約。このステップに続いて、親戚
認識されたリスクのバランスが決定されます。
次に、スパイラルは右下の象限に進みます。
プロジェクトの開発フェーズが始まります。主要なレビュー
各サイクルを完了し、プロセスが新たに開始されます
プロジェクトの後続フェーズ。典型的な後続フェーズは次のとおりです。
ソフトウェア製品の設計、統合、テスト計画の開発、
追加のリスク分析、運用プロトタイプ、詳細設計、

コード、単体テスト、受け入れテスト、および実装。
他の答えは気を散らすものです。

最新問題: **7**
次のうち、オペレーターが実行してはならないものはどれですか？
A. ディスクまたはテープの取り付け
B. バックアップとリカバリ
C. データ入力
D. ハードウェアの取り扱い
Answer: C (メーッセージを残す**)**
これは非常に明白です。オペレーターは、ハードウェアとソフトウェアの実装を処理する運用タスクを作成する責任があり、ハードウェアを処理してユーザーの状態を整え、バックアップと復元の手順を担当し、
バックアップ用のディスクまたはテープのマウント。これらはすべて一般的なタスクです。データ入力について話すとき、作成しなければならないユーザーはそうしますか？オペレーターもそうする場合、ユーザーは何をするつもりですか？

最新問題: **8**
データ所有者（ファイルを作成した人）が所有する情報へのアクセスを制御できるようにするアクセス制御方法はどれですか？
A. DAC-随意アクセス制御
B. MAC-強制アクセス制御
C. RBAC-役割ベースのアクセス制御
D. NDAC-非随意アクセス制御
Answer: A (メーッセージを残す**)**
説明/参照：
Explanation:
DACモデルでのアクセスは、ユーザーに付与された承認に基づいて制限されます。したがって、ユーザーは、所有するオブジェクトに対して発生する可能性のあるアクセスのタイプを識別できます。
不正解：
B：強制アクセス制御（MAC）は、サブジェクトのセキュリティクリアランスとオブジェクトの分類に基づいてオブジェクトへのアクセスを制限するアクセスポリシーです。
C：役割ベースのアクセス制御（RBAC）は、ユーザーが会社内で保持する役割またはユーザーに割り当てられたタスクに応じて、リソースへのアクセスを提供します。
D：非任意アクセス制御とは、システム管理者または組織内の単一の管理機関が、ネットワーク上のすべての人のすべてのリソースへのアクセスを一元的に制御する場合です。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、2013、pp.220-228
http://www.answers.com/Q/What_is_Non_discretionary_access_control

最新問題: **9**
IDおよびアクセスプロビジョニングのライフサイクルの2番目のステップは何ですか？
A. プロビジョニング
B. 失効
C. 承認
D. レビュー
Answer: D (メーッセージを残す**)**

最新問題: **10**
構成管理は何を制御しますか？
A. トラステッドコンピューティングベースへの変更の監査。
B. トラステッドコンピューティングベースへの変更の管理。
C. トラステッドコンピューティングベースへの構成アクセスの変更。
D. トラステッドコンピューティングベースへの変更を監査および制御します。
Answer: D (メーッセージを残す**)**
これらはすべて、構成管理のコンポーネントです。
次の答えは正しくありません。
トラステッドコンピューティングベースへの変更の監査。変更の監査のみを参照し、変更の制御については何も参照していないため、正しくありません。トラステッドコンピューティングベースへの変更の管理。変更を制御することだけを指しているため正しくありませんが、変更がシステムの弱点や障害につながることはありません。トラステッドコンピューティングベースへの構成アクセスの変更。これは、変更を制御したり、変更がシステムの脆弱性や障害につながることがないようにすることを意味しないため、正しくありません。

最新問題: **11**
パケットのデータ構造を指す場合、プロトコルデータユニット PDU）という用語が使用されますが、トランスポート層でTCPデータの単一ユニットを指すのに適切な用語は何ですか？
A. TCPセグメント。
B. TCPデータグラム。
C. TCPフレーム。
D. TCPパケット。
Answer: A (メーッセージを残す**)**
TCPセグメントは、トランスポート層で送信されるTCPデータのグループです。TCP
セグメントベースのネットワークテクノロジーです。
メッセージはトランスポート層に送信され、そこでTCPがデータに魔法をかけます。のバンドルデータはセグメントになりました。メッセージがTCPを介して送信されている場合、それは
"セグメント。"
プロトコルデータユニットレイヤー
次の答えは正しくありません。

TCPデータグラム。TCPデータグラムは気を散らすものにすぎないため、正しくありません。IP
データグラムは
適切な用語。TCPは、セグメントベースのネットワークテクノロジーです。
TCPフレーム。TCPフレームは気を散らすものにすぎないため、正しくありません。イーサネット
フレームは
適切な用語。TCPは、セグメントベースのネットワークテクノロジーです。
TCPパケット。TCPパケットは気を散らすものにすぎないため、正しくありません。TCPは、セグ
メントベースのネットワークテクノロジーです。
この質問に使用される参照：
ウィキペディアhttp://en.wikipedia.org/wiki/Transport_layerウィキペディア
http://en.wikipedia.org/wiki/Transmission_Control_Protocol#TCP_segment_structure
TCP / IP Illustrated、Volume 1 :The Protocols、Addison-
Wesley、1994、ISBN0-201-63346-9。http://www.infocellar.com/networks/osi-model.htm

最新問題: **12**
組織は、追跡を改善するために、資産管理システムにモバイルデバイスを含めることを検討して
います。参照アーキテクチャのどのシステム層でモバイルデバイスを追跡しますか？
A. 1
B. 0
C. 2
D. 3
Answer: B (メーッセージを残す**)**

最新問題: **13**
ANSI ASC X12（米国規格協会認定）
標準化委員会X12）標準バージョン4010は、どちらに適用されますか
次のHIPAAカテゴリの？
A. セキュリティ
B. プライバシー
C. トランザクション
D. コードセット
Answer: (解答を表示する**)**
HIPAAが対応するトランザクションは次のとおりです。
健康強調表示または同様の遭遇情報
医療費の支払いと送金のアドバイス
利益の調整
健康強調表示のステータス
健康保険への加入と加入解除
健康保険の適格性
健康保険料の支払い

紹介の認証と承認
これらのHIPAAに対処するためのHIPAAEDIトランザクション標準
トランザクションには次のものが含まれます。
ヘルスケアの主張または給付の調整
小売薬NCPCP（処方薬のための全国評議会
プログラム）v。32
歯科クレームASCX12N837：歯科
専門家の主張ASCX12N837：専門家
制度的主張ASCX12N837：制度的
支払いと送金のアドバイスASCX12N835
健康強調表示ASCX12N276/277
登録を計画するASCX12834
プランの適格性ASCX12270/271
保険料の支払いを計画するASCX12820
紹介認証ASCX12N 278
米国規格協会は1917年に設立されました
そして、アメリカの標準の唯一の情報源です。ANSI認定
標準委員会X12は1979年に設立され、責任を負っています。
電子文書の業界横断的な基準。HIPAAプライバシー
基準、回答a、2001年4月に最終決定され、実装
2003年4月14日までに達成する必要があります。プライバシールールは
個人を特定できる医療情報が送信されるか、電子形式または紙の形式で保存されるか、口頭で伝達されます。保護された健康情報（PHI）は、開示が承認されない限り開示されない場合があります個人による、法律で許可されている、治療に必要な、ヘルスケア業務の一部、法律で義務付けられている、または支払いに必要な。PHIは、電子メディアによって送信され、HIPAAの下での電子メディアの定義に記載されている任意のメディアで維持される個人を特定できる健康情報として定義されます。
または、他の形式または媒体で送信または維持されます。答え
b、コードセットは、HIPAAトランザクション標準のデータ要素を入力するために使用されるコードを指します。これらのコードの例は次のとおりです。
ICD-9-CM（vol。1および2）国際疾病分類
第9版、臨床修飾疾患、傷害、障害、
その他の健康関連の問題、それらの症状、および
怪我、病気、障害、またはその他の健康関連の問題
CPT（Current Procedural Terminology、4th Ed。[CPT-4]）、CDT
（歯科処置および命名法に関するコード、第2版[CDT-2]）
またはICD-9-CM（vol。3）防止するために取られた手順またはその他のアクション、
病気、怪我、障害を診断、治療、または管理する
NDC（National Drug Codes）薬
HCPCS（Health Care Financing Administration Common

手順コーディングシステム）
その他の健康関連サービス、その他の物質、機器、
消耗品、またはヘルスケアサービスで使用されるその他のアイテム
提案されたHIPAAセキュリティルール、回答dは、
の機密性、完全性、および可用性の保護
保護された健康情報（PHI）：
管理手順
物理的なセーフガード
技術サービスとメカニズム
このルールは電子署名にも対応していますが、最終的なルールは
標準に到達するための業界の進歩に依存します。の
さらに、提案されたセキュリティルールでは、
警備員。

最新問題: **14**
今日のクラッカーは、次のことを望んでいることが最も多いです。
A. コミュニティがネットワークを保護するのを支援します。
B. 彼らのスキルがどれだけ彼らを連れて行くかを見る。
C. 彼らの行動に対する認識を得る。
D. 金銭的利益または金銭的利益の獲得。
Answer: D (メーッセージを残す**)**
説明/参照：
Explanation:
数年前、この質問の最良の選択は、彼らのスキルがどれだけ彼らを連れて行くことができるかを見ることでした。今日、これは大きく変化し、犯された犯罪のほとんどは経済的な動機によるものです。利益は、すべてのサイバー犯罪の背後にある最も広範な動機であり、実際、ほとんどの犯罪–誰もがお金を稼ぎたいと思っています。
金銭や無料サービスのためのハッキングには、横領、企業スパイ、「ハッカーの雇い主」などの犯罪のスモーガスボードが含まれます。詐欺は簡単に実行できますが、成功する可能性ははるかに低くなります。お金を求める人はどんなライフスタイルから来ますが、説得力のあるスキルを持っている人は、非常に技術に精通している人がより良い「雇うためのハック」をするのと同じように、より良い詐欺師を作ります。
「ホワイトハット」は、コミュニティがネットワークを保護するのを支援することに関心のあるセキュリティスペシャリストです（「ブラックハットではありません）。
彼らは所有者の許可を得てシステムとネットワークをテストします。ブラックハットは、攻撃的な目的で自分のスキルを使用する人です。彼らは、適切なセキュリティメカニズムを構成しようとする前に承認を求めません。「グレイハット」とは、ホワイトハットとして働くこともあれば、「ブラックハット」として働くこともある人々であり、どちらの側を好むかについてはまだ決心し

ていません。以下は間違った答えです：他のすべての選択は考えられる理由である可能性がありますが、今日の最良の選択は本当に経済的利益のためです。
参照：
http://library.thinkquest.org/04oct/00460/crimeMotives.html
およびhttp://www.informit.com/articles/article.aspx?p=1160835
http://www.aic.gov.au/documents/1/B/A/%7B1BA0F612-613A-494D-B6C5-06938FE8BB53%7Dhtcb006.pdf

最新問題: **15**
相互認証の主な役割は何ですか？
A. 異なるPKI間の信頼の作成
B. 全体的なPKI階層を構築する
C. 2番目のルートCAへの直接信頼を設定します
D. CA証明書の失効によるユーザー証明書の無効化を防止します
Answer: A (メーッセージを残す**)**
ますます多くの組織が独自の内部PKIを設定しています。これらのとき
独立したPKIは、安全な通信を可能にするために相互接続する必要があります（いずれか
部門間または異なる会社間）、2つのルートCAが信頼する方法が必要です
お互い。
これらの2つのCAには、両方が信頼できるCAが上にないため、クロスを実行する必要があります
認証。相互認証は、信頼関係を確立するためにCAによって行われるプロセスです。
お互いのデジタル証明書と公開鍵を発行したかのように信頼している
彼ら自身。
これを設定すると、ある会社のCAが他の会社のデジタル証明書を検証できます。
およびその逆。
この質問に使用される参照：
相互認証の詳細と図については、以下をご覧ください。
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03qswp.mspx http://www.entrust.com/resources/pdf/cross_certification.pdf
も参照してください：
ション・ハリス、CISSPオールインワンブック、第4版、727ページ
と
RFC 2459 :インターネットX.509公開鍵インフラストラクチャ証明書およびCRLプロファイル。
フォード、ワーウィック＆
BAUM、Michael S.、安全な電子商取引 :デジタル署名のためのインフラストラクチャの構築
and Encryption（2nd Edition）、2000、Prentice Hall PTR、254ページ。

最新問題: **16**
アクセス制御の最大実効コストの決定に最も関連するのは次のうちどれですか？
A. 保護される情報の価値

B. 失われたデータを置き換えるためのコスト
C. 基本支出と増分支出に関連する予算計画。
D. データの重要性に関する経営者の認識
Answer: A (メーッセージを残す**)**

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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**
瞬間的な低電圧として何を定義できますか？
A. スパイク
B.)電圧低下
C. サグ
D. 障害
Answer: C (メーッセージを残す**)**

最新問題: **18**
周囲制御に振動検出装置を使用する場合の一般的な問題は何ですか？
A. 彼らは非敵対的な妨害に対して脆弱です。
B. それらは電子的手段によって打ち負かすことができます。
C. 信号振幅は気象条件の影響を受けます。
D. それらは霜線の下に埋められなければなりません。
Answer: A (メーッセージを残す**)**
振動センサーも同様で、強制侵入を検出するためにも実装されています。金融機関は、銀行強盗が車両を運転しようとする可能性のある外壁にこれらのタイプのセンサーを実装することを選択する場合があります。また、金庫の天井や床の周りで、許可されていない銀行の引き出しを行おうとしている人を検出するためにもよく使用されます。
このようなセンサーは誤検知する傾向があります。重機を搭載した大型トラックが走行している場合、センサーが作動する場合があります。雷と照明のある嵐の場合と同じように、敵対的な脅威や妨害がない場合でも、アラームがトリガーされる可能性があります。
以下は不正解です。
他のすべての選択は正しくありません。
この質問に使用される参照：
ハリス、ション（2012-10-18）。CISSPオールインワン試験ガイド、第6版（pp。495-496）。
マグロウヒル。キンドル版。

最新問題: **19**
Cが情報システムにセーフガードを導入するコストを表す場合
Lは、
対応する脆弱性、セーフガードが
次の場合は実装されません：
A. C /L=定数
B. C> L
C. C <L
D. C = 2L
Answer: (解答を表示する**)**
正解はC<Lです。セーフガードを実装するためのコストが、対応する脆弱性が正常に悪用された場合に発生する推定損失よりも少ない場合、法的責任が存在します。他の答えは気を散らすものです。

最新問題: **20**
組織にとって重要なバックアップ情報は、
A. 脆弱性評価（VA）。
B. 事業継続計画（BCP）。
C. ビジネス影響分析（BIA）。
D. データ回復分析。
Answer: C (メーッセージを残す**)**
セクション :ソフトウェア開発のセキュリティ

最新問題: **21**
実際に多くのソフトウェア開発モデルを組み込んだメタモデルであるソフトウェア開発モデルはどれですか？
A. ウォーターフォールモデル
B. 修正されたウォーターフォールモデル
C. スパイラルモデル
D. クリティカルパスモデル（CPM）
Answer: C (メーッセージを残す**)**
スパイラルモデルは、実際には多くのソフトウェア開発モデルを組み込んだメタモデルです。このモデルは、ソフトウェア開発のさまざまなフェーズを組み込んだスパイラルを表しています。モデルは、スパイラルの各サイクルには、プロジェクトの各部分に対して同じ一連のステップが含まれると述べています。CPMは、クリティカルパス法を指します。出典 :KRUTZ、Ronald L.＆VINES、Russel D.、CISSP Prep Guide :Mastering the Ten Domains of Computer Security、John Wiley＆Sons、2001、Chapter 7 :Applications and Systems Development（246ページ）。

最新問題: **22**

次のステップのうち、ビジネス影響分析（BIA）で最初に実行する必要があるのはどれですか？
A. 組織内のすべてのビジネスユニットを特定します。
B. 破壊的なイベントの影響を評価します。
C. 目標復旧時間（RTO）を見積もります。
D. ビジネス機能の重要性を評価します。
Answer: A (メーッセージを残す)
BIA（Business Impact Analysis）について話すときは、インフラストラクチャで発生する可能性のある問題を分析および特定していることを忘れないでください。これは、ビジネス、それが中継するプロセス、システムのレベル、および財務上の影響の見積もり、つまり、システムがダウンした状態でどれだけ多くを失うかについての分析です。その最初のステップは、常に会社のビジネスユニットを特定することです。次に、損失の見積もりやダウンタイムコストなどの他の要件に進むことができます。

最新問題**: 23**
組織の情報セキュリティ管理を開発する際に従うことが最も重要なのは、次のうちどれですか？
A. すべての国内および国際規格を確認し、場所に基づいて最も厳しいものを選択します。
B. 組織のセキュリティ管理に業界標準のベストプラクティスを使用します。
C. 適切な管理を調整するために、すべてのリスク管理情報に関してデューデリジェンスを実行します。
D. リスク評価を実行し、既存のギャップに対処する基準を選択します。
Answer: B (メーッセージを残す)

最新問題**: 24**
事業継続計画を作成する際、タイムクリティカルなシステムを特定して優先順位を付ける責任があるのは次のうち誰ですか？
A. 経営幹部
B. シニアビジネスユニット管理
C. BCP委員会
D. 機能的なビジネスユニット
Answer: B (メーッセージを残す)
説明/参照：
Explanation:
上級管理職は最終的に計画のすべての段階に責任があり、誰がその資産の保護について最も心配する必要があります。彼らはすべてのポリシーの問題を承認する必要があり、セキュリティソリューションの全体的な成功または失敗に対して責任を負います。
不正解：
A：可能であれば、BCP計画は経営幹部によって承認されるべきですが、経営幹部はタイムクリティカルなシステムを特定して優先順位を付ける責任を負いません。
C：BCP委員会は、システムを特定して優先順位を付けていません。BCP委員会は、BCPを監督、開始、計画、承認、テスト、および監査します。また、BCPを実装し、活動を調整し、BIA調査を承認し

ます。BCP委員会はまた、継続計画の作成を監督し、品質保証活動の結果をレビューします。D：機能的なビジネスユニットはBCP委員会の一部です。機能的なビジネスユニットは、タイムクリティカルなシステムを特定して優先順位を付ける責任を負いません。
参照：
Stewart、James M.、Ed Tittel、およびMike Chapple、CISSP：Certified Information Systems Security Professional Study Guide、第5版、Sybex、インディアナポリス、2011年、p。55

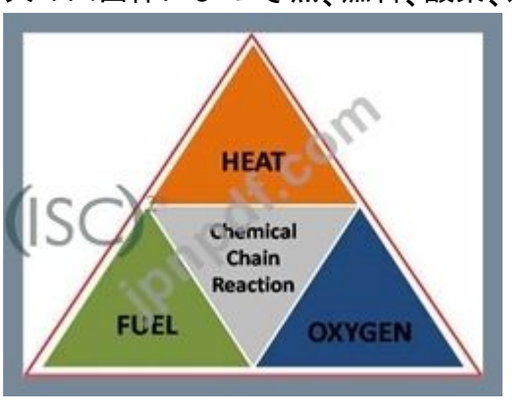
最新問題: **25**
ハイブリッド暗号化を使用してセッションキーを伝達するキー配布プロトコルとして最も適切に定義できるのは、次のうちどれですか。このプロトコルは、長期キーを一度確立し、その後、セッションごとにキーを確立または交換するために事前の通信を必要としませんか？
A. インターネットセキュリティアソシエーションおよびキー管理プロトコル（ISAKMP）
B. インターネットプロトコルの単純なキー管理（SKIP）
C. Diffie-Hellman鍵配布プロトコル
D. IPsecキー交換（IKE）
Answer: B (メーッセージを残す**)**
RFC 2828（インターネットセキュリティ用語集）では、インターネットプロトコルの単純なキー管理（SKIP）を次のように定義しています。
ハイブリッド暗号化を使用して、IPパケット内のデータの暗号化に使用されるセッションキーを伝達するキー配布プロトコル。
SKIPは、SSLと同様のハイブリッドキー配布プロトコルですが、長期キーを1回確立し、セッションごとにキーを確立または交換するために事前の通信を必要としない点が異なります。したがって、接続設定のオーバーヘッドは存在せず、新しいキー値は継続的に生成されません。SKIPは、独自の秘密鍵または秘密コンポーネントと宛先の公開コンポーネントの知識を使用して、それらの間でのみ使用できる一意の鍵を計算します。
IKEはInternetKeyExchangeの略で、ISAKMPとOAKLEYを内部で利用します。
インターネットキーエクスチェンジ（IKEまたはIKEv2）は、セキュリティアソシエーション（SA）を設定するために使用されるプロトコルです。
IPsecプロトコルスイート。IKEは、OakleyプロトコルとISAKMPに基づいて構築されています。IKEはX.509を使用します
認証用の証明書と共有セッションを設定するためのDiffie-Hellman鍵交換
暗号化キーの派生元の秘密。
以下は不正解です。
ISAKMPは、セキュリティをネゴシエート、確立、変更、および削除するためのインターネットIPsecプロトコルです。
関連付け、および詳細に関係なく、キーの生成と認証データを交換する
特定の鍵生成技術、鍵確立プロトコル、暗号化アルゴリズム、または
認証メカニズム。
IKEは、インターネット、IPsec、キー確立プロトコル（一部はOAKLEYに基づく）であり、

ISAKMPで使用するため、およびその他のセキュリティのために、認証されたキー情報を配置するため
AHやESPなどの関連付け。
IPsecキー交換（IKE）は、単なる欠点です。
この質問に使用される参照：
SHIREY、Robert W.、RFC2828：Internet Security Glossary、2000年5月。
と
http://en.wikipedia.org/wiki/Simple_Key-Management_for_Internet_Protocol
と
http://en.wikipedia.org/wiki/Simple_Key-Management_for_Internet_Protocol

最新問題: **26**
S / MIME規格ではどのような暗号化が実現されていますか？
A. 非対称暗号化方式
B. パスワードベースの暗号化スキーム
C. 公開鍵ベースのハイブリッド暗号化スキーム
D. 楕円曲線ベースの暗号化
Answer: C (メーッセージを残す**)**
S / MIME（Secure MIME、またはSecure Multipurpose Mail Extensionの場合）はセキュリティです
電子メール交換に使用されるプロセスで、機密性と非機密性を保証することができます。
電子メッセージの否認。
S / MIMEはMIME標準に基づいており、その目的はユーザーが以外のファイルを添付できるようにすることです。
電子メッセージへのASCIIテキストファイル。したがって、MIME標準により、添付が可能になります。
電子メールへのすべてのタイプのファイル。
S / MIMEは、もともとRSADataSecurity社によって開発されました。1999年7月に
IETF、S / MIMEが標準になり、その仕様はRFC2630から2633に含まれています。
S/MIMEのしくみ
S / MIME標準は、公開鍵暗号化の原則に基づいています。したがって、S/MIMEは
メッセージの内容を暗号化することは可能ですが、通信を暗号化することはできません。
MIME標準に従ってエンコードされた、電子メッセージのさまざまなセクションは次のとおりです。
それぞれがセッションキーを使用して暗号化されています。
セッションキーは各セクションのヘッダーに挿入され、受信者のパブリックを使用して暗号化されます
鍵。受信者だけが自分の秘密鍵を使用してメッセージの本文を開くことができます。これにより、受信したメッセージの機密性と完全性。
さらに、メッセージの署名は送信者の秘密鍵で暗号化されます。誰
通信を傍受すると、メッセージの署名の内容を読み取ることができますが、これにより、

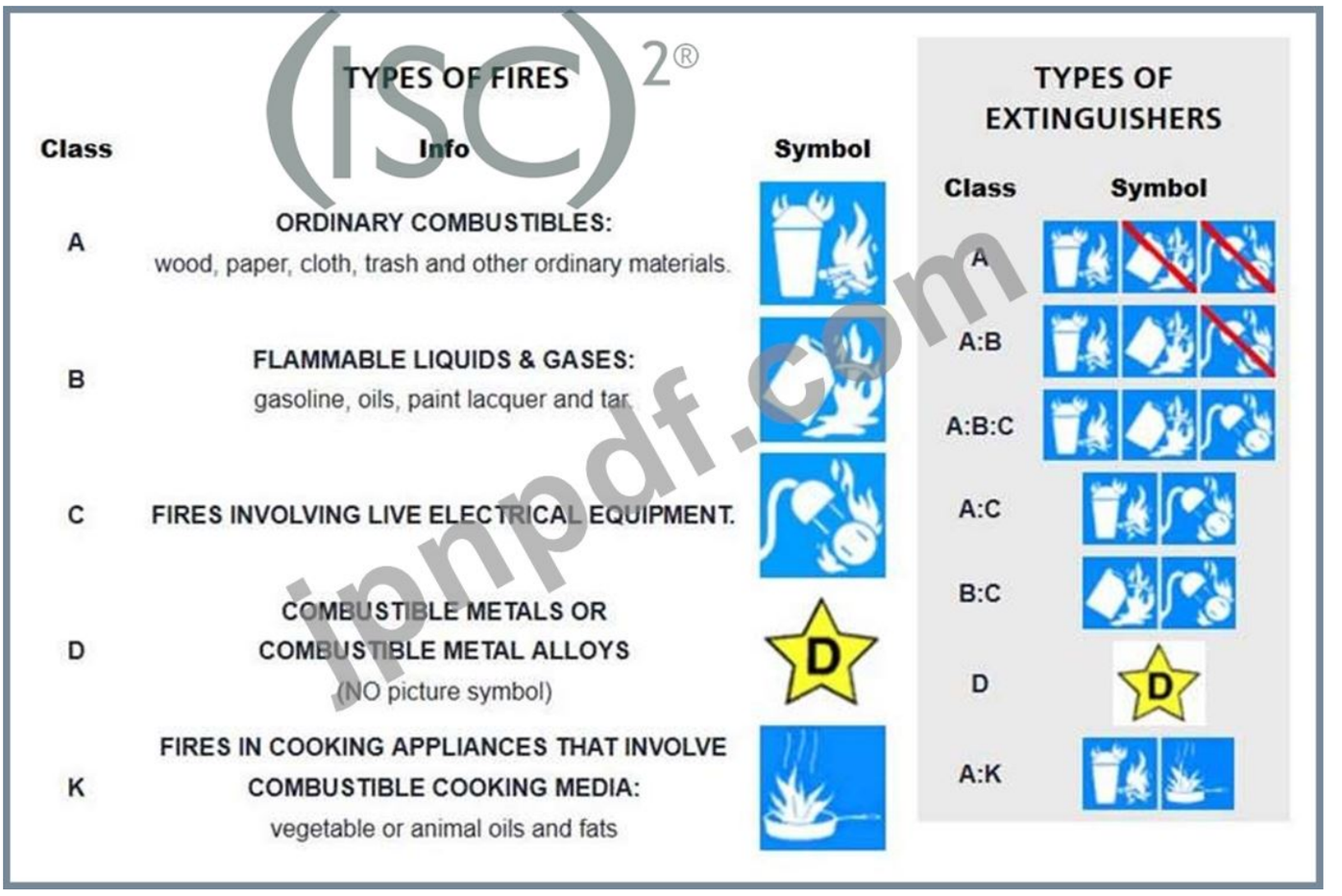
送信者のみがメッセージを暗号化できるため、送信者のIDの受信者
（彼の秘密鍵を使用して）彼の公開鍵を使用して復号化できます。
この質問に使用される参照：
http://en.kioskea.net/contents/139-cryptography-s-mime
RFC 2630：暗号化メッセージ構文;
OPPLIGER、Rolf、PGPおよびS / MIMEを使用したセキュアメッセージング、2000、Artech House;
HARRIS、ション、オールインワンCISSP認定試験ガイド、2001年、McGraw-Hill / Osborne、ページ
570;
SMITH、Richard E.、Internet Cryptography、1997、Addison-Wesley Pub Co.

最新問題: **27**
火の4つの基本的な要素は何ですか？
A. 熱、燃料、酸素、連鎖反応
B. 熱、燃料、CO2、連鎖反応
C. 熱、木材、酸素、連鎖反応
D. 炎、燃料、酸素、連鎖反応
Answer: A (メーッセージを残す**)**
火が存在するためには、4つの要素が存在する必要があります。これらの要素はHEATです。
燃料、酸素および連鎖反応。
燃焼プロセスについてすべてが知られているわけではありませんが、火は一般的に受け入れられています
化学反応。この反応は、急速に酸化する、または
酸素が非常に急速に発生するため、熱と炎が発生します。
新しい消火剤が登場するまで、火は3つの三角形であると考えられていました。
熱、燃料、および酸素によって表される側面。3つの側面のいずれかが削除された場合、
火は存在しなくなります。
現代の消火剤の研究により、4番目の要素である自己増殖が明らかになりました
燃焼過程における連鎖反応。その結果、火の基本的な要素が表されます
火の四面体によって熱、燃料、酸素、連鎖反応。



火の四面体

消火の理論は、火を抑制するために、火の四面体の4つの要素のいずれか1つまたは複数を削除することに基づいています。
熱を取り除く熱を取り除くには、火に何かを当てて熱を吸収するか、熱交換器として機能させる必要があります。これを達成するために使用される薬剤は水だけではありませんが、最も一般的です。
燃料の除去多くの状況下で、火から燃料を除去しようとすることは現実的ではありません。可燃性液体の火災に対処する場合、バルブを遮断し、貯蔵容器を安全な場所にポンプで送って、火災への燃料の供給をなくすことができます。可燃性ガスの火災は、燃料の供給を遮断することで完全に消火されます。
酸素を取り除く私たちの大気中に存在する酸素（21%）は、ほとんどの火災状況での燃焼をサポートするのに十分です。空気または酸素の除去は、燃料源から分離するか、不活性ガスで置き換えることによって達成できます。分離の例としては、引火性液体の火の泡、ゴミの火の濡れた毛布、フライパンの火のぴったりと合う蓋などがあります。CO2、窒素、蒸気などの薬剤は、酸素を置換するために使用されます。
連鎖反応を中断する
ドライケミカルやハロンなどの最新の消火剤は、
これらの薬剤は熱、燃料、または酸素を除去しませんが、さまざまな火災が発生します。ドライケミカルと
ハロゲン化剤は、で生成される「フリーラジカル」を懸濁または結合すると考えられています
燃焼プロセス、したがってそれらが連鎖反応を継続するのを防ぎます。
現在、ハロンはほとんどの国または都市で禁止されていることに注意する必要があります。ハロンを禁止する協定
生産はモントリオール議定書と呼ばれています。
次のリンクをクリックして、消火剤と消火剤に関するすばらしいビデオをご覧ください。
試験のために知っておく必要のある情報。
火のクラスの再開：



火災のクラス
他のすべての答えは正しくありません：
参考資料：消火および消火およびhttp://code7700.com/fire.html

最新問題: **28**
事業継続計画（BCP）をテストするためのベストプラクティスは次のうちどれですか？
A. セキュリティパッチのインストール後にテストする
B. システムパッチの実装後にテストする
C. IT監査の前にテストする
D. 環境が変化したときにテストする
Answer: D (メーッセージを残す**)**

最新問題: **29**
プログラムを介してのみオブジェクトへのアクセスを導入するセキュリティモデルはどれですか？
A. ビバモデル
B. ベルラパドゥラモデル
C. クラークウィルソンモデル
D. 情報フローモデル
Answer: C (メーッセージを残す**)**

Clark-Wilsonモデルでは、サブジェクトはオブジェクトに直接アクセスできなくなりましたが、代わりにプログラム（整形式のトランザクション）を介してオブジェクトにアクセスする必要があります。
Clark-Wilson整合性モデルは、コンピューティングシステムの整合性ポリシーを指定および分析するための基盤を提供します。
このモデルは、主に情報の整合性の概念を形式化することに関係しています。
エラーまたは悪意によるシステム内のデータ項目の破損を防ぐことにより、情報の整合性が維持されます。整合性ポリシーは、システム内のデータ項目をシステムのある状態から次の状態まで有効に保つ方法を説明し、システム内のさまざまなプリンシパルの機能を指定します。モデルは、施行規則と認証規則を定義します。
Clark-Wilsonは、情報コンテンツの整合性があらゆるレベルの分類で最も重要であるビジネスおよび業界のプロセスにより明確に適用できます。
Clark-Wilsonモデルの整合性の目標：
許可されていないユーザーによる変更を防止します（これのみがビバモデル）。
職務の分離は、許可されたユーザーが不適切な変更を行うことを防ぎます。
整形式のトランザクション：内部および外部の一貫性を維持します。つまり、データをある一貫性のある状態から別の状態に転送するために実行される一連の操作です。
以下は不正解です。
ビバモデルが正しくありません。Bibaモデルは整合性に関係しており、サブジェクトのセキュリティレベルとオブジェクトのセキュリティレベルの比較に基づいてオブジェクトへのアクセスを制御します。
Bell-LaPdaulaモデルが正しくありません。Bell-LaPaulaモデルは機密性に関係しており、対象のクリアランスレベルとオブジェクトの分類レベルの比較に基づいてオブジェクトへのアクセスを制御します。
情報フローモデルが正しくありません。情報フローモデルは、オブジェクトがセキュリティクラスでラベル付けされ、情報が上向きまたは同じレベルで流れることができるラティスを使用します。フレームワークはベルラパドゥラモデルに似ています。
参照：
ISC2公式学習ガイド、325～327ページ
AIO3、pp.284-287
AIOv4セキュリティのアーキテクチャと設計（338～342ページ）
AIOv5セキュリティアーキテクチャと設計（341～344ページ）
ウィキペディア：https://en.wikipedia.org/wiki/Clark-Wilson_model

最新問題: **30**
ネットワークベースのログは、被害者のマシンに関する悪意のあるアクティビティを確認するときに、ホストベースのログよりも優れていますか？
A. ネットワークベースのログのアドレスとプロトコルが分析されます。
B. ホストベースのシステムロギングでは、ファイルが複数の場所に保存されています。

C. 適切に処理されたネットワークベースのログは、より信頼性が高く、有効である可能性があります。
D. ネットワークベースのシステムは、コンソールにログインしているユーザーをキャプチャできません。
Answer: (解答を表示する**)**
セクション :ソフトウェア開発のセキュリティ

最新問題**: 31**
情報の適切なアクセス制御を誰が決定する必要がありますか？
A. オーナー
B. ユーザー
C. 管理者
D. サーバー
Answer: A (メーッセージを残す**)**
生成または使用されるすべての情報には、指定された所有者が必要です。所有者は、適切な感度分類とアクセス制御を決定する必要があります。所有者はまた、情報の保管、処理、配布、および使用を安全に管理するための適切な管理を確実にするための措置を講じる必要があります。

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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**
伝聞証拠に対する事業免除規則の下で、次の例外のうち、法廷での監査ログおよび監査証跡の不許可に関係がないのはどれですか？
A. 記録は通常の業務中に収集されます。
B. 記録は上級管理職または経営幹部によって収集されます。
C. 記録は、自動化されたレポートを生成するために、調査対象の行為の発生時またはその近くに収集されます。
D. 収集されたレコード/データ/ログを誰も変更できなかったことを証明できます。
Answer: (解答を表示する**)**
伝聞証拠は、コンピューターログを生成して収集したビジネスパーソンのように、証拠の正確性、信頼性、信頼性を証明するために使用できる直接の証拠がない限り、通常は法廷で許容されません。
この人物が、法廷での1回だけではなく、通常の業務の一部としてログを生成および収集することが重要です。それは、毎日実行される文書化されたプロセスでなければなりません。

証拠の価値は、情報源の信憑性と能力に依存します。したがって、記録の収集は上級管理職または経営幹部によって実行される可能性が高い活動ではないため、上級管理職または経営幹部によって収集された記録は法廷で許容されない可能性があります。
伝聞証拠は通常、伝聞証拠の業務記録免除規則を満たさない限り、法廷で許容されません。
場合によっては、コンピューターの記録が伝聞規則の範囲外になります（例：業務記録の免除）
情報は通常の事業活動に関連しています
自動的にコンピューターで生成されたデータ
人間の介入なし
システムが正しく動作していたことを証明する
誰もデータを変更していないことを証明する
文書化されたビジネスプロセスがあり、侵入検知ツールを使用している場合は、ログに記録します
分析ツールを使用し、アクティビティの日次レポートを作成すると、コンピューターで生成されたデータが
法廷で許容され、伝聞証拠とは見なされません。
この質問に使用される参照：
HARRIS、ション、オールインワンCISSP認定試験ガイド、McGraw-Hill / Osborne、2002年、章10：法、調査、および倫理（676ページ）。

最新問題: **33**
次の説明のうち、IPSecトランスポートモードに当てはまるものはどれですか。最良の2つを選択してください。
A. ゲートウェイ間通信で使用する場合、ゲートウェイはホストとして機能する必要があります
B. エンドポイントがホストの場合、またはエンドポイントで通信が終了する場合に設定できます
C. 探偵/管理ペアリング
D. 内部システムへのアクセスを提供するゲートウェイに必要です
Answer: A,B (メーッセージを残す**)**

最新問題: **34**
次のうち、レイヤー2トンネリングプロトコル（L2TP）インターネットプロトコルセキュリティ（IPSec）接続内にエンドツーエンドのセキュリティを追加するのはどれですか？
A. Temporal Key Integrity Protocol（TKIP）
B. セキュアハッシュアルゴリズム（SHA）
C. セキュアシェル（SSH）
D. トランスポート層セキュリティ（TLS）
Answer: B (メーッセージを残す**)**
セクション :ソフトウェア開発のセキュリティ

最新問題: **35**

組織は、クラウドベースのサービスプロバイダーと契約して、サービス提供としてのアイデンティティを活用することを決定しました。彼らはOpenAuthentication（OAuth）2.0を使用して、組織のサービスに対して外部ユーザーを認証します。
認証プロセスの一環として、エンドユーザーが提供する必要があるのは次のうちどれですか？
A. アクセストークン
B. パスワード
C. ユーザー名とパスワード
D. ユーザー名
Answer: A (メーッセージを残す**)**

最新問題**: 36**
アクセス制御の機密性の側面をキャプチャするステートマシンモデルは次のうちどれですか？
A. クラークウィルソン
B. ベルラパドゥラ
C. チャイニーズウォール
D. ラティス
Answer: B (メーッセージを残す**)**
Bell-LaPadulaは、アクセス制御の機密性の側面を捉えたステートマシンモデルです。アクセス許可は、アクセス制御マトリックスおよびセキュリティレベルの半順序によって定義されます。セキュリティポリシーは、情報が高いセキュリティレベルから低いセキュリティレベルに下がるのを防ぎます。BLPは、サブジェクトがオブジェクトを観察または変更したときに発生する情報フローのみを考慮します。

最新問題**: 37**
ホットサイト施設とは何ですか？
A. 配線が事前に設置され、フリーアクセスフロアでスペースが確保されているサイトです。
B. コンピューターがプリインストールされたサイト、上げ床、エアコン、電気通信、ネットワーク機器、およびUPS
C. 通信機器、LAN、PC、およびワークグループを備えた端末を備えた既製のワークスペースを備えたサイト
D. 上げ床、空調、通信、ネットワーク機器、およびUPSを備えたサイト
Answer: B (メーッセージを残す**)**

最新問題**: 38**
営業秘密に関する次の記述のうち、間違っているものはどれですか？
A. 営業秘密法は通常、リソースのアイデアの表現を保護します。
B. 企業が企業秘密として適格なリソースを持つためには、企業に何らかの競争力のある価値または利点を提供する必要があります
C. 多くの企業は、企業秘密の保護に関する機密保持契約に署名することを従業員に要求しています

D. リソースが一般的に知られていない場合、およびリソースを開発するために特別なスキル、創意工夫、および/またはお金と労力の支出が必要な場合、リソースは法律によって保護できます。
Answer: A (メーッセージを残す**)**

最新問題**: 39**
次のプロトコルのどれがセッション層（層）で動作しますか？
A. RPC
B. IGMP
C. 自民党
D. SPX
Answer: A (メーッセージを残す**)**
ネットワーク使用のソケット方式はメッセージベースのシステムであり、あるプロセスが別のプロセスにメッセージを書き込みます。これは、手続き型モデルからは遠い道のりです。
リモートプロシージャコールは、プロシージャコールのように機能することを目的としていますが、ネットワーク全体で透過的に機能します。プロセスは、パラメータとリターンアドレスをスタックにプッシュし、プロシージャの先頭にジャンプすることで、リモートプロシージャコールを実行します。手順自体は、ネットワークへのアクセスと使用を担当します。
リモート実行が終了すると、プロシージャはリターンアドレスにジャンプして戻ります。
その後、呼び出しプロセスが続行されます。RPCは、OSIモデルのセッション層で機能します。

最新問題**: 40**
指紋認証プロセス中に、IDと認証を検証するために使用されるのは次のうちどれですか？
A. 圧力値が保存されているテンプレートと比較されます
B. 特徴点のテンプレートが保存されているテンプレートと比較されます
C. ハッシュテーブルがプリペイドのデータベースと照合されます
D. 数字のセットは保存された値と一致します
Answer: B (メーッセージを残す**)**

最新問題**: 41**
単純なネットワーク端末がLAN経由でサーバーからオペレーティングシステムをロードできるようにするための単純なメカニズムとして開発されたのは、次のうちどれですか？
A. DHCP
B. BootP
C. DNS
D. ARP
Answer: B (メーッセージを残す**)**
BootPは、単純なネットワーク端末がLAN経由でサーバーからオペレーティングシステムをロードできるようにするための単純なメカニズムとして開発されました。時間の経過とともに、ネットワーク上のホストのIDと動作の多くの側面を一元的に構成できるように拡張されました。より複雑なDHCPが、時間の経過とともにBootPに取って代わったことに注意してください。出典：

STREBE、Matthew and PERKINS、Charles、Firewalls 24seven、Sybex 2000、第4章 :セキュリティの観点からのソケットとサービス。

最新問題: **42**
次の個人のうち、セキュリティを実装するシステム上のソフトウェアにアクセスするのは、 職務の分離」の原則に違反しますか？
A. セキュリティ管理者
B. セキュリティアナリスト
C. システム監査人
D. システムプログラマー
Answer: D (メーッセージを残す**)**
理由 :セキュリティ管理者、セキュリティ分析、およびシステム監査者は、職務を遂行するためにセキュリティシステムの一部にアクセスする必要があります。システム ・プログラマーは、動作中の（別名：実動）セキュリティー ・システムにアクセスする必要はありません。
プログラマーは、実行中のコンピューターに継続的に直接アクセスすることを許可されるべきではありません
生産システム（組織が事業を運営するために使用するシステム）。維持する
システムの整合性、本番システムに加えた変更は、
組織の変更管理制御システム。
セキュリティ管理者の仕事はセキュリティ機能を実行することであるため、
セキュリティタスクは厳密に制限する必要があります。この職務の分離により、損失の可能性が減少します。
割り当てられた機能の範囲外でアクションを実行することにより、ユーザーが権限を悪用した結果
責任。
参照：
OFFICIAL (ISC)2 @ GUIDE TO THE CISSP @ EXAM (2003)、Hansche、S.、Berti、J.、Hare、H.、Auerbach Publication、FL、Chapter 5-Operations Security、section 5.3、"Security Technology and ツール」、 人事」セクション (32ページ)。
KRUTZ、R. &VINES、R. CISSP Prep Guide :Gold Edition (2003)、Wiley Publishing Inc.、
第6章：運用セキュリティ、職務の分離 (303ページ)。

最新問題: **43**
IPSecで、通信がゲートウェイからゲートウェイまたはホストからゲートウェイになる場合：
A. トンネル動作モードが必要です
B. トランスポートモードのみ使用できます
C. カプセル化セキュリティペイロード (ESP）認証を使用する必要があります
D. トンネルモードとトランスポートモードの両方を使用できます
Answer: A (メーッセージを残す**)**

エンポイントがホストの場合、トランスポートモードが確立されます。ゲートウェイ間通信のゲートウェイがトランスポートモードを使用する場合、それはホストシステムとして機能します。これは、そのゲートウェイへの直接プロトコルで受け入れられます。それ以外の場合は、ゲートウェイサービスにTUNNELモードが必要です...これは最も一般的な動作モードであり、ゲートウェイからゲートウェイおよびホストからゲートウェイへの通信に必要です。
出典 :TIPTON、Harold F.&KRAUSE、MICKI、情報セキュリティ管理
ハンドブック、第4版、第2巻、2001年、CRC Press、ニューヨーク、167ページ。

最新問題: **44**
知っておくべきことの最良の定義は、次のうちどれですか？
A. 知る必要があるのは、オペレーターが自分のタスクを実行するために必要なシステムについての最低限の知識を持っていることです。
B. 知っておく必要があることにより、（単独で行動する）1人の個人がセキュリティ管理を危険にさらすことはありません。
C. 知っておくべきことは、各ユーザーにタスクに必要な最低のクリアランスを付与します。
D. 知る必要があると、オペレーターがタスクを実行する時間が制限されます。
Answer: A (メーッセージを残す**)**
知る必要があるという概念は、何にでも加えて、
ユーザーがシステム上で持つ可能性のある特定のオブジェクトまたはロールの権利、
ユーザーは、実行するために必要な最小限の情報も持っています
彼の職務。
*回答 「知っておく必要があることで、（一人で行動する）1人の個人がセキュリティ管理を危険にさらすことはありません。」職務の分離であり、タスクの一部を異なる担当者に割り当てます。
*回答 「知る必要があると、各ユーザーにタスクに必要な最低のクリアランスが付与されます。」最小特権の場合、ユーザーは自分の職務を実行するために必要な最小のセキュリティレベルを持っています。
*回答 「知る必要があると、オペレーターがタスクを実行する時間が制限されます。」職務のローテーションであり、オペレーターにセキュリティに敏感なタスクが割り当てられる時間は、異なるセキュリティ分類を持つ別のタスクに移動する前に制限されます。

最新問題: **45**
国防総省のマルチレベルの軍事安全保障政策を抽象的な正式な言葉で最初に説明したのは誰ですか？
A. デビッド・ベルとレナード・ラパドゥラ
B. リベスト、シャミール、エーデルマン
C. ホイットフィールドディフィーとマーティンヘルマン
D. デビッド・クラークとデビッド・ウィルソン
Answer: A (メーッセージを残す**)**
説明/参照：

Explanation:
1973年に、国防総省のマルチレベルの軍事安全保障政策を抽象的な正式な用語で最初に説明したのは、DavidBellとLeonardLaPadulaでした。Bell-LaPadulaは、機密性に関係する強制アクセス制御（MAC）モデルです。Rivest、Shamir、およびAdleman（RSA）は、RSA暗号化アルゴリズムを開発しました。WhitfieldDiffieとMartinHellmanは、1976年にDiffie-Hellman鍵合意アルゴリズムを公開しました。DavidClarkとDavid Wilsonは、商業活動のセキュリティにより適したClark-Wilson整合性モデルを開発しました。
参考資料：RUSSEL、Deborah＆GANGEMI、GT Sr.、Computer Security Basics、O'Reilly、1992年7月（78、109ページ）。

最新問題: **46**
組織内でセキュリティポリシーを有効にするには、セキュリティポリシーに次のものを含める必要があります。
A. コンプライアンス違反に対する懲戒処分。
B. ポリシーに適用されるすべての標準のリスト。
C. 問題を明確に定義する強力なステートメント。
D. 所有者情報と最終改訂日。
Answer: (解答を表示する**)**

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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**
マルチレベルセキュリティをデータベース管理システムに後付けするために一般的に使用されるのは次のうちどれですか？
A. 信頼できるフロントエンド
B. 信頼できるバックエンド
C. コントローラー
D. カーネル
Answer: A (メーッセージを残す**)**
説明/参照：
Explanation:
マルチレベルセキュリティ（MLS）データベースシステムでは、信頼できるフロントエンドが構成されます。ユーザーは信頼できるフロントエンドに接続し、信頼できるフロントエンドはデータベースシステムに接続します。

信頼できるフロントエンドは、クエリを正しいデータベースプロセッサに送信し、データベースプロセッサ間で不正な情報の流れがないことを確認し、レプリケートされたデータベースフラグメント間のデータの一貫性を維持し、クエリ応答に適切なラベルを付けてに送信する責任があります。適切なユーザー。さらに、信頼できるフロントエンドは、ユーザーの識別と認証、ユーザーへの信頼できるパスの保守、および監査を担当します。
不正解：
B：信頼できるバックエンドが構成されていません。バックエンドはデータベースシステムになります。ユーザーは信頼できるフロントエンドに接続し、フロントエンドはバックエンドデータベースシステムに接続します。
C：ロントローラー」は、マルチレベルセキュリティデータベースシステム用に構成されたシステムの正しい用語ではありません。
D :カーネルはオペレーティングシステムの心臓部です。これは、マルチレベルセキュリティデータベースシステム用に構成されたものではありません。
参照：
http://www.acsac.org/secshelf/book001/19.pdf

最新問題**: 48**
アクセス制御の用語で、 支配する」という言葉は、次のうちどれを指しますか？
A. アクセスクラス以上
B. 権利は優先されます
C. 読み取り権限を持つ有効な知っておくべきこと
D. 他のユーザーよりも高いクリアランスレベル
Answer: A (メーッセージを残す**)**
アクセスクラス以上。その理由は、 支配する」という用語は、サブジェクトのアクセスクラスがより高いか、要求されたオブジェクトのアクセスクラスを支配する場合に、操作を実行することを許可されているサブジェクトを指すためです。これがその用語の最良の答えです
アクセス制御で 支配」します。
被験者がオブジェクトにアクセスしたい場合、彼のセキュリティクリアランスは彼がアクセスしているオブジェクトと同じかそれ以上でなければなりません。
次の答えは正しくありません。
実際には有効な条件ではないため、権利が優先されます。
読み取り権限を持つ有効な知る必要性は、特定的すぎて支配的ではなく、通常、ユーザーのラベルが示すものです。
他よりも高いクリアランスレベル。より高いレベルのデータにアクセスするには、より高いクリアランスレベルを持つことが重要かもしれませんが、それは
支配する」とは、アクセス制御を指します。
この質問を作成するために、次の参照が使用されました。
ション・ハリス最新の オールインワンCISSP試験準備」280ページ。

最新問題: **49**
フリーカーは、電話詐欺を専門とするハッカーです。フリーダイヤルの電話を受けるために線間電圧を操作する電話詐欺の種類は何ですか？
A. ブラックボックス
B. 白いボックス
C. 青いボックス
D. 赤いボックス
Answer: A (メーッセージを残す**)**

最新問題: **50**
質問に答えるには、以下の情報を参照してください。
セキュリティインシデントの調査中に、許可されていない個人が財務情報を含むデータベースをホストするシステムにアクセスしたと判断されました。
侵入によってシステムプロセスがハングした場合、影響を受けたのは次のうちどれですか？
A. システムの可用性
B. システムの機密性
C. システムの監査可能性
D. システムの整合性
Answer: A (メーッセージを残す**)**

最新問題: **51**
OSIアーキテクチャモデルのレイヤーではないものはどれですか？
A. データリンク
B. インターネット
C. 輸送
D. セッション
Answer: B (メーッセージを残す**)**
正解はインターネットです。インターネット層は、TCP/IPアーキテクチャモデル層です。

最新問題: **52**
IPヘッダーにはプロトコルフィールドが含まれています。このフィールドに値1が含まれている場合、IPデータグラムにはどのタイプのデータが含まれていますか？
A. TCP。
B. ICMP。
C. UDP。
D. IGMP。
Answer: (解答を表示する**)**
プロトコルフィールドの値が1の場合、それはICMPであったことを示します。
次の答えは正しくありません。
TCP。TCPプロトコルの値は6になるため、正しくありません。

UDP。UDPプロトコルの値は17になるため、正しくありません。
IGMP。IGMPプロトコルの値は2になるため、正しくありません。

最新問題: **53**
ファイルがバックアップされた後、通常、どのバックアップ方法がファイルのアーカイブビットをリセットしますか？
A. 増分バックアップ方式。
B. 差分バックアップ方式。
C. 部分バックアップ方式。
D. テープバックアップ方式。
Answer: A (メーッセージを残す**)**
説明/参照：
Explanation:
増分バックアップ方式は、最後の完全バックアップまたは増分バックアップ以降に変更されたすべてのファイルをバックアップし、アーカイブビットを0にリセットします。これは「アーカイブビットのクリア」と呼ばれます。フルバックアップは、アーカイブビットが1であるか0であるかに関係なく、すべてのファイルをバックアップし、アーカイブビットを0に設定します。
アーカイブビットは、ファイルが変更されたかどうかを判断するためにバックアッププロセスによって使用されます。ファイルを変更するか、新しいファイルを作成すると、アーカイブビットが1に設定されます。これにより、バックアッププロセスに、ファイルが変更された（または新しいファイルである）ため、バックアップする必要があることが通知されます。増分バックアップがファイルをバックアップするとき、アーカイブビットを0に設定します。次の増分バックアップが実行され、アーカイブビットが0であることを確認すると、増分バックアップは、ファイルが最後のバックアップ以降に変更されていないことを認識します。ファイルを再度バックアップします。
不正解：
B：差分バックアップ方式では、前回の完全バックアップ以降に変更されたファイルのみがバックアップされます。
このバックアップ方法では、アーカイブビットはリセットされません。
C：部分バックアップ方式は、アーカイブビットをリセットするかどうかを決定する方式ではありません。データのサブセットがバックアップされることを指定するだけです。
D：テープバックアップ方式は、アーカイブビットがリセットされているかどうかを判断する方式ではありません。ファイルがテープにバックアップされることを指定するだけです。
参照：
Krutz、Ronald L. and Russel Dean Vines、CISSP Prep Guide：Mastering the Ten Domains of Computer Security、John Wiley＆Sons、New York、2001、p。69

最新問題: **54**

オープンシステム相互接続（OSI）モデルのどの層が他の層に依存しており、情報の構造、解釈、および処理に関係していますか？
A. プレゼンテーション層
B. セッション層
C. トランスポート層
D. アプリケーション層
Answer: A (メーッセージを残す**)**

最新問題**: 55**
次のうち、ハッキングベクトルとしてのリモートアクセスサーバーを介したダイヤルアップアクセスを最も効果的に排除できるのはどれですか？
A. TACACS+サー バーを使用します。
B. ファイアウォールの外側にリモートアクセスサーバーをインストールし、正当なユーザーにファイアウォールへの認証を強制します。
C. モデムの呼び出し回数を5以上に設定する
D. ネットワークに接続されていないホストにのみモデムを接続します。
Answer: B (メーッセージを残す**)**
説明/参照：
Explanation:
クライアントコンピュータにはインターネット接続を可能にするモデムが組み込まれていたため、組織は通常、ネットワークへのリモートアクセスとネットワークからのリモートアクセスを可能にするモデムのプールを持っていました。場合によっては、モデムはネットワーク全体のあちこちにある個々のサーバーにインストールされているか、中央に配置されて管理されていました。ほとんどの企業は、これらのモデム接続を介したアクセス制御を適切に実施しておらず、攻撃者にとって簡単なエントリポイントとして機能していました。
リモートアクセスサーバーをファイアウォールの外側にインストールし、正当なユーザーにファイアウォールへの認証を強制することで、ハッキングベクトルとしてのリモートアクセスサーバーを介したダイヤルアップアクセスを排除するのが最善です。このソリューションは、攻撃者がリモートアクセスサーバーにアクセスした場合でも、ファイアウォールが別の保護レイヤーを提供することを意味します。
不正解：
A :TACACS +サーバーを使用すると、優れたリモートアクセス認証および承認ソリューションが提供されます。
ただし、リモートアクセスサーバーを介したダイヤルアップアクセスをハッキングベクトルとして排除するには、リモートアクセスサーバーをファイアウォールの外側に配置する必要があります。
C :モデムの呼び出し回数を少なくとも5に設定すると、監視員を阻止できますが、ハッキングベクトルとしてのリモートアクセスサーバーを介したダイヤルアップアクセスを排除することはできません。

D :ネットワークに接続されていないホストにモデムを接続するだけでは、ハッキングベクトルとしてのリモートアクセスサーバーを介したダイヤルアップアクセスが排除されません。非実用的であることに加えて、非ネットワークホストは攻撃に対して脆弱です。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、2013、p。695

最新問題: **56**
組織の異種エンドポイントネットワークに制御を実装する場合、次のことが重要です。
A. ユーザーはセキュリティソフトウェアの構成を変更できます。
B. 各ホストで実行されているファイアウォールはユーザーが完全にカスタマイズできます。
C. ホストはネットワーク通信を確立できます。
D. 共通のソフトウェアセキュリティコンポーネントがすべてのホストに実装されています。
Answer: (解答を表示する**)**

最新問題: **57**
災害の結果について最も正確な説明は次のうちどれですか
回復計画テスト？
A. テストの結果に関係なく、計画を変更しないでください。
B. テスト中に欠陥が見つからなかった場合、計画はおそらく完璧です。
C. テストの結果は秘密にしておく必要があります。
D. テスト中に欠陥が見つからなかった場合は、テストに欠陥がある可能性があります。
Answer: D (メーッセージを残す**)**
テストの目的は、計画の弱点を見つけることです。すべての計画には弱点があります。テスト後、すべての関係者に結果を通知し、新しい情報を反映するように計画を更新する必要があります。

最新問題: **58**
モデムとダイヤルアップリモートアクセスシステムの基本言語は次のとおりです。
A. 非同期通信。
B. 同期通信。
C. 非同期相互作用。
D. 同期相互作用。
Answer: (解答を表示する**)**
説明/参照：
Explanation:
非同期スタートストップは、データリンクフレーミングプロトコルを使用して、多くのダイヤルアップインターネットアクセスアプリケーションのモデムにコンピューターを接続するために使用される物理層です。
不正解：
B :ダイヤルアップモデムは、同期ではなく非同期の通信を使用します。
C :ダイヤルアップモデムは、対話ではなく通信を使用してリモートシステムに接続します。

D :ダイヤルアップモデムは、対話ではなく通信を使用してリモートシステムに接続します。
参照：
https://en.wikipedia.org/wiki/Asynchronous_serial_communication

最新問題: **59**
侵入テスト中に、組織内の全員が機密データを保持しているサーバーに不正アクセスしていることが明らかになった場合に、システム管理者が最初に実行する必要があるアクションは次のうちどれですか。
A. 調査結果を直ちに文書化し、上級管理職に報告します。
B. 侵入テストを終了し、サーバー管理チームに調査結果を渡します
C. システム権限を使用して、サーバーを保護するための権限を変更します
D. テストを最後まで続けてから、IT管理者に通知します
Answer: A (メーッセージを残す**)**

最新問題: **60**
異なる実行ドメイン内の特定のサブジェクトが使用できるオブジェクトの範囲を制限するために使用されるPRIMARYメカニズムは次のうちどれですか？
A. プロセスの分離
B. データの隠蔽と抽象化
C. ディスクリートレイヤリングとアプリケーションプログラミングインターフェイス（API）の使用
D. 仮想プライベートネットワーク（VPN）
Answer: A (メーッセージを残す**)**

最新問題: **61**
質問に答えるには、以下の情報を参照してください。
新しい従業員には、完全な管理者アクセス権を持つラップトップコンピューターが与えられます。この従業員は自宅にパソコンを持っておらず、そのパソコンを使って電子メールの送受信、Webの検索、インスタントメッセージングを使用する子供がいます。組織の情報技術（IT）部門は、従業員のアクセスを使用してピアツーピアプログラムがコンピューターにインストールされていることを発見しました。
コンピュータからピアツーピア（P2P）プログラムを削除する最も効果的な方法は、次のうちどれですか？
A. ウェブブラウザのキャッシュに保存されているすべてのCookieを削除します
B. すべてのインストールファイルを見つけて削除します
C. ソフトウェアのアンインストールを実行します
D. コンピューターのイメージを再作成します
Answer: (解答を表示する**)**

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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**
以下のどのプロトコルが電子メールに関係しませんか？
A. SMTP
B. CHAP
C. POP
D. IMAP
Answer: B (メーッセージを残す**)**
チャレンジハンドシェイク認証プロトコル（CHAP）は、リモートリンクの起動時にリモートノードのIDを確認するために使用されます。
* Simple Mail Transfer Protocol（RFC 821および1869）は、インターネットを介して電子メールを配信するためにサーバーによって使用されます。
* Post Office Protocol（RFC 1939）を使用すると、ユーザーはリモートサーバーからローカルコンピューターに電子メールをダウンロードして、電子メールを読むことができます。
*インターネットメッセージアクセスプロトコル（RFC 2060）を使用すると、ユーザーはメールをローカルにダウンロードしなくても、リモートサーバーでメールを読むことができます。出典：Eoghan Caseyが編集したコンピュータ犯罪調査ハンドブック（Academic Press、2002年）。

最新問題: **63**
次のうち、クラスBの火災に適切な抑制媒体ではないものはどれですか？
A. ハロン
B. 水
C. ソーダ酸
D. CO2
Answer: (解答を表示する**)**
正解は水です。水はクラスBの火災の適切な抑制媒体ではありません。他の3つは一般的に使用されます。

最新問題: **64**
ジョブローテーションは次の理由で重要です。
A. それはあなたの従業員が相互訓練されることを保証します。
B. 仕事の満足度が上がります。
C. 詐欺の機会を減らします
Answer: (解答を表示する**)**

ジョブローテーションは、最小特権の原則と密接に関連しています。効果的なセキュリティ管理です。

最新問題: **65**
周囲制御に振動検出装置を使用する場合の一般的な問題は何ですか？
A. 彼らは非敵対的な妨害に対して脆弱です。
B. それらは電子的手段によって打ち負かすことができます。
C. 信号振幅は気象条件の影響を受けます。
D. それらは霜線の下に埋められなければなりません。
Answer: A (メーッセージを残す**)**
振動センサーも同様で、強制侵入を検出するためにも実装されています。金融機関は、銀行強盗が車両を運転しようとする可能性のある外壁にこれらのタイプのセンサーを実装することを選択する場合があります。また、金庫の天井や床の周りで、許可されていない銀行の引き出しを行おうとしている人を検出するためにもよく使用されます。
このようなセンサーは誤検知する傾向があります。重機を搭載した大型トラックが走行している場合、センサーが作動する場合があります。雷と照明の嵐と同じように、それは警報を引き起こすかもしれません
あなたでさえ、敵対的な脅威や妨害はありません。
以下は不正解です。
他のすべての選択は正しくありません。
この質問に使用される参照：
ハリス、ション（2012-10-18）。CISSPオールインワン試験ガイド、第6版（pp。495-496）。マグロウヒル
。キンドル版。

最新問題: **66**
すべての不正な変更または実行の干渉からプログラムを保護するために何が使用されますか？
A. 保護ドメイン
B. セキュリティ境界
C. セキュリティラベル
D. 抽象化
Answer: A (メーッセージを残す**)**
保護ドメインは、各プロセスに割り当てられた実行スペースとメモリスペースで構成されます。保護ドメインを確立する目的は、すべての不正な変更または実行の干渉からプログラムを保護することです。セキュリティ境界は、Trusted Computing Base（TCB）をシステムの残りの部分から分離する境界です。分類のタイプを示すために、セキュリティラベルがリソースに割り当てられます。抽象化は、システムコンポーネントを高レベルで表示し、その特定の詳細を無視して情報の隠蔽を実行するという事実から、リソースを保護する方法です。出典：KRUTZ、Ronald L.＆VINES、Russel D.、CISSP Prep Guide：Mastering the Ten Domains of Computer Security、John Wiley＆Sons、2001、Chapter 5：Security Architecture and Models（193ページ）。

最新問題: **67**
オブジェクト指向システムにおいて、共通のオブジェクトを持つ状況
名前は、一般的な一連の操作に対して異なる方法で応答します。
A. ポリインスタンス化。
B. 委任。
C. ポリレスポンス。
D. ポリモーフィズム。
Answer: D (メーッセージを残す**)**
委任とは、あるオブジェクトから別のオブジェクトへの要求の転送です。
回答ポリレスポンスは気を散らすものです。
ポリインスタンス化は、詳細バージョンの開発です
別のオブジェクトからのオブジェクトの。新しいオブジェクトは、次の値を使用します
元のオブジェクトのものとは異なります。

最新問題: **68**
次のうち、Secure Sockets Layer（SSL）に当てはまらないものはどれですか？
A. 慣例により、「http ://」の代わりに「s-http ://」を使用します。
B. トランスポート層セキュリティ（TLS）プロトコルの前身です。
C. Netscapeによって開発されました。
D. インターネットを介して個人情報、データ、およびドキュメントを送信するために使用されます。
Answer: A (メーッセージを残す**)**
SSLを使用するWebページは、「http ://」ではなく「https ://」を使用しますが、
Secure-httpを使用します。s-http ://で始まります。
次の答えは正しくありません。
トランスポート層セキュリティの前身であり、Netscapeによって開発され、
インターネットを介してプライベートドキュメントを送信する。
これらはすべて真の答えであるため、この質問には正しくありません。
参考資料 :TIPTON、Harold F.＆HENRY、Kevin、Official（ISC）2 Guide to the CISSP CBK、2007、496、976ページ
KRUTZ、Ronald L.＆VINES、Russell Dean、The CISSP Prep Guide、Gold Edition、2003、117ページ

最新問題: **69**
攻撃者はどのようにしてスタックオーバーフローを悪用して任意のコードを実行することができますか？
A. スタックポインタを移動します
B. スタックのアドレスを変更します。

C. 関数のリターンアドレスを変更します。
D. スタック内の要素を置き換えます。
Answer: C (メーッセージを残す**)**

最新問題**: 70**
次のうち、リスク管理の結果を知識を持って使用できるようにするのに最適なものはどれですか？
A. 脆弱性分析
B. 尤度評価
C. 不確実性分析
D. 脅威の特定
Answer: C (メーッセージを残す**)**
リスク管理は、2つの主要な活動と1つの根本的な活動で構成されています。リスク評価とリスク軽減が主要な活動であり、不確実性分析が根本的な活動です。リスク評価と軽減を実行した後、不確実性分析を実行する必要があります。リスク管理は、多くの場合、推測、最良の推測、不完全なデータ、および多くの証明されていない仮定に依存する必要があります。文書化された不確実性分析により、リスク管理の結果を知識を持って使用することができます。脆弱性分析、可能性評価、脅威の特定はすべて、リスク管理の主要な活動の1つである、リスク評価のデータ部分の収集と分析の一部です。
出典：SWANSON、Marianne＆GUTTMAN、Barbara、National Institute of Standards、Technology（NIST）、NIST Special Publication 800-14、一般的に受け入れられている原則および情報技術システムを保護するための慣行、1996年9月（9〜21ページ）。

最新問題**: 71**
財務担当のDebbieは、無料の壁紙プログラムをダウンロードしてインストールし、現在の外の天気に合わせて壁紙を設定しましたが、コンピューターの動作が遅くなり、ディスクドライブのアクティビティライトが常に点灯していることを伝えました。よく見ると、単純なポートスキャンを実行して、彼女のコンピューターで開いているポートを確認すると、TCP/80が開いていることがわかります。彼女のコンピューターのIPアドレスとポートにWebブラウザーを向けると、処方薬を販売しているサイトが表示されます。
壁紙変更ソフトウェアとは別に、デビーは知らないうちに何をインストールしましたか？
A. トロイの木馬
B. ネットワークモバイルコード
C. ウイルス
D. 論理爆弾
Answer: (解答を表示する**)**
説明/参照：
Explanation:
トロイの木馬は、有用なアプリケーションを装ったコードですが、悪意のある、または有害な目的が埋め込まれたコードが含まれています。トロイの木馬は、バックドアの設定、キーストロークロ

ガーのインストール、ルートキットの実装、被害者のシステムからのファイルのアップロード、ボットソフトウェアのインストール、その他多くの種類の悪意のある行為を実行できます。
不正解：
B :ネットワークモバイルコードは通常、ワームと呼ばれます。これは、ワームが悪用する脆弱性に対してパッチが適用されていない隣接するホストに感染する悪意のあるソフトウェアです。
C :ウイルスは、自分自身のコピーをそのプログラムに埋め込むことによって、自分自身をホストプログラムに添付するコードのセグメントです。ウイルスがデビーのコンピューターにポートを開いたり、処方薬を販売するサイトをインストールしたりすることはありません。
D：論理爆弾は、特定の条件が満たされたときに一連の命令を実行します。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、New York、2013、pp.1199-1201、
1202、1206
http://en.wikipedia.org/wiki/Trojan_horse_(computing）

最新問題**: 72**
サルベージチームによって青信号が出された後、プライマリサイトで通常の操作を再開する手順について話すとき、以下の最も正しい選択は何ですか？
A. 最も重要な操作は、他のサイトよりも先に代替サイトからプライマリサイトに移動されます
B. ディザスタリカバリチームとはまったく異なるチームが運用を行う場合があります
C. 最も重要度の低い機能を最初に戻す必要があります
D. 計画内のカテゴリドキュメントと同じ順序で、または代替サイトへの途中で行ったのとまったく同じ順序でアイテムを戻します。
Answer: C (メーッセージを残す**)**
通常の処理操作を再開する手順は、復旧計画の手順とは異なることに注意してください。つまり、最も重要度の低い作業を最初にプライマリサイトに戻す必要があります。
上記の手順で最も重要なポイントは、最も重要度の低いアイテムまたはリソースを最初にプライマリサイトに戻すことです。このようにして、サイトが本当によく準備されていて、すべてが正常に機能していることを確認できます。
その最初のステップが完了する前に、サルベージチームから、プライマリサイトに戻っても問題がないことを示す緑色のライトが表示されます。緑色のライトを取得した後の最初のステップは、最も重要度の低い要素を最初に移動することです。
ション・ハリスの本で述べられているように、最も重要度の低い機能を最初に戻す必要があります。そのため、ネットワーク構成や接続に問題がある場合、または重要な手順が実行されなかった場合でも、会社の重要な業務に悪影響はありません。最も重要なシステムと操作を安全で安定したサイトに移動し、テストされていないメインサイトに戻すだけの問題を経験するのはなぜですか？重要度の低い部門をカナリアとして機能させます。それらが生き残った場合は、会社のより重要なコンポーネントに移動します。

会社が元のサイトまたは新しいサイトに戻る時期になると、会社は再構成フェーズに入ります。会社は、バックアップ施設での運用中は常に脆弱であるため、元のプライマリサイトまたはプライマリサイトを置き換えるために構築された新しいサイトで運用を再開するまで、緊急状態から抜け出すことはありません。
会社が代替サイトから元のサイトにいつ戻る必要があるかについては、多くのロジスティクスの問題を考慮する必要があります。以下に、これらの問題のいくつかを示します。
従業員の安全の確保
適切な環境が提供されていることを確認する（電力、施設インフラストラクチャ、水、HVAC）
必要な機器と備品が存在し、正常に機能していることを確認する
適切な通信および接続方法が機能していることを確認する
新しい環境を適切にテストする
コーディネーター、管理者、およびサルベージチームが施設の準備を承認したら、サルベージチームは次の手順を実行する必要があります。
代替サイトからデータをバックアップし、新しい施設内で復元します。
不測の事態の操作を慎重に終了します。
機器と人員を新しい施設に安全に輸送します。
他のすべての選択は正しい答えではありません。
この質問に使用される参照：
ハリス、ション（2012-10-25）。CISSPオールインワン試験ガイド、第6版（Kindleの場所19389）。マグロウヒル。キンドル版。
と
KRUTZ、Ronald L.＆VINES、Russel D.、CISSP Prep Guide：Mastering the Ten Domains of Computer Security、John Wiley＆Sons、2001、290ページ。

最新問題: **73**
データが継続的に送信され、内部クロッキングソースまたはタイミングの開始/停止ビットを使用しないデータ伝送方法は、次のように知られています。
A. 非同期
B. 準同期
C. 同期
D. アイソクロナス
Answer: (解答を表示する**)**
アイソクロナスデータは、クロックソースなしで送信する同期データであり、ビットは継続的に送信され、スタートビットまたはストップビットはありません。すべてのビットは同じ重要性であり、一定の時間間隔で発生すると予想されます。
*非同期は、データ値の先頭にスタートビットを使用し、値の末尾にストップビットを使用するデータ伝送方式です。
* synchronousは、データ送信の速度に合わせてクロッキングパルスを使用するメッセージフレーム送信方式です。

* pleisiochronousは、複数のタイミングソースを使用する送信方法であり、異なる速度で実行される場合があります。この方法では、マスタークロックデバイスとスレーブクロックデバイスが必要になる場合があります。出典：RayHorakによるCommunicationsSystems and Networks（M&T Books、2000）。

最新問題: **74**
ソフトウェア開発ライフサイクル（SDLC）では、ハードウェアとソフトウェアの正確なインベントリを維持することが、
A. 品質保証。
B. システム統合。
C. リスク管理。
D. 変更管理。
Answer: D (メーッセージを残す**)**

最新問題: **75**
次の組み合わせのうち、可用性に最も悪影響を与えるのはどれですか？
A. 火災およびデータの偶発的な変更
B. サービス拒否（DoS）攻撃と古いハードウェア
C. 不正なトランザクションとサービス拒否攻撃
D. 不正な取引と古いハードウェア
Answer: (解答を表示する**)**

最新問題: **76**
次の信頼サービスの原則のうち、サードパーティプロバイダーの顧客に提供されるシステム、製品、またはサービスによって使用される情報のアクセス可能性に言及しているのはどれですか？
A. セキュリティ
B. プライバシー
C. アクセス
D. 可用性
Answer: D (メーッセージを残す**)**
可用性とは、エンティティのシステムで使用される情報、および顧客に提供される製品やサービスへのアクセス可能性を指します。可用性の目標自体は、許容可能な最小のパフォーマンスレベルを設定するものではありません。システム機能（システムが実行する特定の機能）またはユーザビリティ（特定のタスクまたは問題のパフォーマンスにシステム機能を適用するユーザーの能力）には対応していません。ただし、運用、監視、および保守のためのアクセシビリティをサポートするための制御がシステムに含まれているかどうかについては取り上げています。

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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**
情報資産の分類を決定する際に考慮すべき最良の基準は、次のうちどれですか？
A. 値
B. 年齢
C. 耐用年数
D. 個人的な協会
Answer: A (メーッセージを残す**)**
説明/参照：
Explanation:
情報資産の「価値」は、情報資産を分類するために使用する必要があります。
さまざまな種類のデータに値を割り当てる理由は、すべてのデータが企業にとって同じ価値を持つわけではないため、企業が各種類のデータを保護するために必要な資金とリソースの量を測定できるようにすることです。すべての重要な情報を特定した後、それを適切に分類する必要があります。会社には、作成および維持される多くの情報があります。データを分類する理由は、データの損失、開示、または入手不能に対する感度に応じてデータを整理するためです。データが機密レベルに従ってセグメント化されると、企業はさまざまな種類のデータを保護するために必要なセキュリティ制御を決定できます。これにより、情報資産が適切なレベルの保護を受けることが保証され、分類によってそのセキュリティ保護の優先順位が示されます。
不正解：
B：情報資産の年齢は、情報資産の分類を決定する際に考慮すべき最良の基準ではありません。
C：情報資産の耐用年数は、情報資産の分類を決定する際に考慮すべき最良の基準ではありません。
D：情報資産の個人的な関連付けは、情報資産の分類を決定する際に考慮すべき最良の基準ではありません。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、New York、2013、p。109

最新問題**: 78**
ハニーポットを設置する主な目的は何ですか？
A. ハッカーを誘惑して未使用のシステムを攻撃させる
B. 可能性のあるハッカーを捕らえて追跡する
C. ネットワーク上に犠牲の子羊を設置する

D. 特定の種類の攻撃がいつ進行中であるかを知り、ネットワークを強化できるように攻撃手法について学ぶこと。
Answer: (解答を表示する**)**
ハニーポットの主な目的は、攻撃者の攻撃方法を理解し、防御を強化する目的で、攻撃者の攻撃方法を研究することです。
「ハッカーを誘惑して未使用のシステムを攻撃させる」は正しくありません。ハニーポットはおとりとして機能することができますが、その主な目的は攻撃者の行動を研究することです。
「可能性のあるハッカーを捕らえて追跡する」は正しくありません。誘惑と罠には多くの法的な問題がありますが、一般的には罠は禁止されており、攻撃者を「罠にかける」と見なされる可能性のあるシナリオで収集された証拠は法廷で許容されません。
「ネットワーク上に犠牲の子羊を設置すること」は正しくありません。ハニーポットは一種の犠牲的な子羊であり、実動システムに対して向けられた可能性のある攻撃を引き付ける可能性がありますが、その本当の目的は、ネットワーク防御をよりよく理解して改善することを目的として、攻撃者の方法を研究することです。
参照：
AIO3、p。213

最新問題: **79**
情報技術セキュリティ評価基準（ITSEC）は、オレンジブックが取り上げていない次のどれに対処するために作成されましたか？
A. 完全性と機密性。
B. 機密性と可用性。
C. 整合性と可用性。
D. 上記のどれでもない。
Answer: (解答を表示する**)**
TCSECは機密性に重点を置き、ITSECは次のように整合性と可用性を追加しました。
セキュリティの目標。
次の答えは正しくありません。
完全性と機密性。TCSECが機密性に対処したため、正しくありません。
機密性と可用性。TCSECが機密性に対処したため、正しくありません。
上記のどれでもない。ITSECがセキュリティ目標として整合性と可用性を追加したため、正しくありません。

最新問題: **80**
次のうち、デューデリジェンスの概念に違反しないものはどれですか？
A. セキュリティポリシーが古くなっています
B. データ所有者がデータ保護の基盤を提示していない
C. ネットワーク管理者が計画どおりに2週間の休暇をとっていない
D. パッチ管理プロセスに従ってインストールされているサーバーの最新のセキュリティパッチ

Answer: D (メーッセージを残す)
効果的にするには、パッチ管理プログラムを実施する必要があり（デューデリジェンス）、詳細な手順で、パッチを適切に適用する方法と時期を指定します（デューケア）。デューデリジェンスの違反ではないという質問をしたことを忘れないでください。この場合、パッチの適用はデューデリジェンスを示し、パッチ管理プロセスは適切なデューデリジェンスを示します。
デューデリジェンスとは、会社が直面するリスクを調査して理解する行為です。企業は、セキュリティポリシー、手順、および標準を開発および実装することによって実践しています。リスクの検出は、ISO 2700、ベストプラクティスなどの標準、およびNIST標準などの他の公開された標準に基づいています。
デューデリジェンスは、現在の脅威とリスクを理解しています。デューデリジェンスは、リスクが絶えず評価およびレビューされている場合に、保護メカニズムが継続的に維持され、運用可能であることを確認する活動によって実施されます。セキュリティポリシーが古くなっていることは、デューデリジェンスの概念に違反している例です。
Due Careは、これらの脅威からの保護を提供するための対策を実施しています。十分な注意を払うのは、特定された可能性のあるリスクから会社とそのリソースを保護するために必要な手順です。情報所有者がデータ保護の基盤を構築せず（それについて何かをする）、指示が実施されていることを確認しない場合（実際に行われ、許容可能なレベルに保たれている）、これは適切なケアの概念に違反します。
会社がその資産のセキュリティに関して十分な注意とデューデリジェンスを実施しない場合、その会社は法的に過失で起訴され、その過失の影響について責任を問われる可能性があります。責任は通常、デューデリジェンスとデューケアまたはどちらかの欠如に基づいて確立されます。
これを覚えておくための良い方法は、デューデリジェンス内の両方の単語の最初の文字を使用することです
（DD）およびDue Care（DC）。
デューデリジェンス=デューディテクト
ベストプラクティスと基準に基づいてリスクを特定するために実行する手順。
デューケア=デューコレクト。
リスクレベルを許容レベルまで下げ、そのレベルを長期にわたって維持するために実行するアクション。
次の答えは間違っていました：
セキュリティポリシーが古くなっています：
セキュリティポリシーを設定して適用することは正しいことですが（デューデリジェンス）、セキュリティポリシーが古くなっている場合は、正しい方法で実行していません（デューデリジェンス）。この質問は、デューデリジェンスに違反し、十分な注意には違反しません。
データ保護の基盤を構築していないデータ所有者：
データ所有者は、「正しいこと」を認識していません。彼らはセキュリティポリシーを持っていません。
ネットワーク管理者は必須の2週間の休暇を取っていません：

2週間の休暇は 正しいこと」ですが、休暇を取らないことはデューデリジェンスに違反します（正しいことを正しい方法で行わないこと）
この質問に使用される参照：
ション・ハリス、CISSPオールインワン、バージョン5、第3章、110ページ

最新問題: **81**
システム開発ライフサイクル $DLC）の次のフェーズのうち、緊急時対応計画が最も重要なのはどれですか？
A. 印心
B. 開発/買収
C. 実装
D. 運用/保守
Answer: (解答を表示する**)**
説明/参照：
Explanation:
システム開発ライフサイクル $DLC）は、情報システムを開発するプロセスです。SDLCには、開始、開発、取得、実装、運用、保守、および廃棄の各フェーズが含まれます。
開始フェーズには、システムの目標と実現可能性の決定が含まれます。システムの実現可能性には、システム要件と、それらが運用プロセスとどの程度一致しているかが含まれます。緊急時対応計画の要件は、システムの要件と設計に基づいて分析する必要があります。
不正解：
B：緊急時対応計画は、開発/取得フェーズではなく、開始フェーズで最も重要です。プロジェクトの可能な限り早い段階で緊急時対応計画を作成することが重要です。
C：緊急時対応計画は、実装フェーズではなく、開始フェーズで最も重要です。緊急時対応計画は、システムを実装する前に作成する必要があります。
D：緊急時対応計画は、運用/保守フェーズではなく、開始フェーズで最も重要です。システムが展開された後ではなく、プロジェクトの可能な限り早い段階で緊急時対応計画を作成することが重要です。
参照：
EC-Council、Disaster Recovery、Cengage Learning、Andover、2010年、4〜11ページ

最新問題: **82**
管理者によるシステムの全体的なセキュリティの妥当性の正式な承認とは何ですか？
A. 認証
B. 受け入れ
C. 認定
D. 評価
Answer: C (メーッセージを残す**)**
認定とは、本番環境にソフトウェアまたはシステムを実装するための管理者による承認です。この承認は、暫定的または完全なもののいずれかです。

以下は不正解です。
認定が正しくありません。認証は、のセキュリティスタンスを評価するプロセスです。
選択した一連の標準またはポリシーに対するソフトウェアまたはシステム。認定は技術的なものです
製品の評価。これは認定に先行する可能性がありますが、必須の前兆ではありません。
受け入れが正しくありません。この用語は、ソフトウェアの一部または
システムは一連の機能レベルまたはサービスレベルの基準を満たしています（新しい給与システムは
検収試験）。この文脈では、認証がより良い方法です。
評価が正しくありません。評価は確かに認証プロセスの一部ですが、そうではありません
質問に対する最良の答え。
この質問に使用される参照：
ISC2のCBKの公式学習ガイド、559～560ページ
AIO3、pp.314-317
AIOv4セキュリティのアーキテクチャと設計（369～372ページ）
AIOv5セキュリティアーキテクチャと設計（370～372ページ）

最新問題: **83**
次のうち、従業員がインシデントを報告するのを妨げる可能性が低いのはどれですか？
A. 彼らは関与したくない何かに引き込まれることを恐れています。
B. インシデントの報告プロセスは一元化されています。
C. 彼らは自分たちがしなかったことで非難されることを恐れています。
D. 彼らは会社のセキュリティポリシーと手順を知りません。
Answer: B (メーッセージを残す**)**
説明/参照：
Explanation:
一元化されたインシデント報告は、従業員がインシデントを報告する可能性を減らすのではなく、増やすでしょう。
不正解：
A：従業員は、関与することを恐れ、インシデントの報告を控えることができます。
C：自分がしなかったことで告発されることを恐れている従業員は、事件を報告する可能性が低くなります。
D：会社のセキュリティポリシーと手順を知らない従業員は、インシデントを報告する可能性が低くなります。
参照：
https://en.wikipedia.org/wiki/Computer_security_incident_management

最新問題: **84**
次のベストのうち、システムへのアクセスがフェデレーションユーザーアカウントにどのように許可されるかを説明しているのはどれですか？

A. フェデレーション保証レベル
B. アイデンティティ保証レベル
C. IDプロバイダー（IdP）によって定義された基準に基づく
D. 依拠当事者（RP）によって定義された基準に基づく
Answer: C (メーッセージを残す**)**

最新問題**: 85**
次の質問のうち、監査証跡をカバーする統制の評価に役立つ可能性が最も低いのはどれですか？
A. 監査証跡はユーザーアクションのトレースを提供しますか？
B. インシデントは解決されるまで監視および追跡されますか？
C. オンラインログへのアクセスは厳密に管理されていますか？
D. アクセス制御機能を管理するセキュリティ担当者と監査証跡を管理するセキュリティ担当者の間に職務の分離はありますか？
Answer: B (メーッセージを残す**)**
監査証跡は、システムまたはアプリケーションプロセスごとのシステムアクティビティの記録を維持します
そしてユーザーの活動によって。適切なツールと手順と組み合わせて、監査証跡は提供することができます
個人の説明責任、イベントを再構築し、侵入を検出し、問題を特定する手段。
監査証跡管理は技術管理と見なされます。インシデントの監視と追跡はもっと
インシデント対応機能に関連する運用管理。
この質問に使用される参照：
SWANSON、Marianne、NIST Special Publication 800-26、セキュリティ自己評価ガイド
情報技術システム、2001年11月（ページA-50からA-51）。
注：NIST SP 800-26は次のように置き換えられました：FIPS 200、SP 800-53、SP 800-53A新しい代替品は次の場所にあります：http：//csrc.nist.gov/publications/PubsSPs.htmlただし、あなたは本当に古い標準を見たいと思っています、それはアーカイブされた文書としてリストされています：http://csrc.nist.gov/publications/PubsSPArch.html

最新問題**: 86**
相互認証を使用する分散ファイルシステムのセキュリティは、マルチユーザーホストのファイルセキュリティとどのように異なりますか？
A. アクセス制御はオペレーティングシステム（OS）に依存できず、盗聴
B. アクセス制御はオペレーティングシステム（OS）に依存できますが、盗聴は
C. アクセス制御はオペレーティングシステム（OS）に依存できず、盗聴
D. アクセス制御はオペレーティングシステム（OS）に依存でき、盗聴は
Answer: D (メーッセージを残す**)**

最新問題**: 87**

国際機関は、その事業運営をサポートするためにサービスとしてのソフトウェア（SaaS）ソリューションを使用することを決定しました。ソリューションの国際的なコードセキュリティとデータプライバシーを評価するために、組織は次のコンプライアンス基準のどれを使用する必要がありますか？
A. サービス組織管理（SOC）2
B. 情報保証技術フレームワーク（IATF）
C. 医療保険の相互運用性と説明責任に関する法律（HIPAA）
D. ペイメントカード業界（PCI）
Answer: A (メーッセージを残す**)**

最新問題**: 88**
GSMでは認証はどのように実装されていますか？
A. 公開鍵暗号を使用する
B. GSMには実装されていません
C. 秘密鍵暗号化の使用
D. 帯域外検証
Answer: C (メーッセージを残す**)**
認証は、共通の使用を通じてGSMで実行されます
ネットワークオペレータの認証に保存されている秘密鍵Ks
センター（AuC）および加入者のSIMカード。SIMカードが入っている可能性があります
加入者のラップトップであり、加入者はKsに精通していません。認証交換を開始するために、加入者のモバイルステーションのホームロケーション（MS）は、128ビットの乱数（RAND）を生成します。
それをMSに送信します。両方のAuCに知られているアルゴリズムを使用する
MSの場合、RANDは、秘密鍵を使用して両方の当事者によって暗号化されます。
Ks。次に、MSで生成された暗号文がAuCに送信され、
Aucによって生成された暗号文と比較して。2つの結果が
一致すると、MSが認証され、アクセス要求が許可されます。もしも
それらが一致しない場合、アクセス要求は拒否されます。したがって、他の答えは正しくありません。

最新問題**: 89**
最近組織を離れた同僚が、セキュリティの専門家に組織の機密インシデント管理ポリシーのコピーを要求しました。このリクエストに対する最良の回答は次のうちどれですか？
A. 会社が発行したデバイスのポリシーにアクセスし、元の同僚に画面を表示させます。
B. 会社の公式チャネルを使用してリクエストを送信し、ポリシーの配布に問題がないことを確認します。
C. 元同僚からの依頼を受けたことを認めず、無視してください。
D. 同僚はすでに組織の一部であり、それに精通しているため、ポリシーを同僚に電子メールで送信します。

Answer: C (メーッセージを残す)

最新問題**: 90**
写真を識別したり、その真正性を検証したりするために使用されるステガノグラフィの商用アプリケーションとは何ですか？
A. MAC
B. デジタルチェックサム
C. MD5ハッシュ
D. デジタル署名
E. 透かし
Answer: E (メーッセージを残す)
透かしは、写真を識別したり、その真正性を検証したりするために使用されるステガノグラフィの商用アプリケーションです。

最新問題**: 91**
異常検出IDSが多数の誤検知を生成することが多いのはなぜですか？
A. 彼らはすでに知っている攻撃しか正しく識別できないからです。
B. アプリケーションベースであるため、攻撃を受けやすくなります。
C. 異常な行動を特定できないため。
D. ユーザーとシステムの通常の動作パターンは大きく異なる可能性があるためです。
Answer: (解答を表示する)
説明/参照：
Explanation:
異常ベースの侵入検知システムは、システムアクティビティを監視し、それを正常または異常に分類することにより、コンピュータの侵入と誤用を検出するためのシステムです。分類は、パターンやシグニチャではなく、ヒューリスティックまたはルールに基づいており、通常のシステム操作から外れるあらゆるタイプの誤用を検出しようとします。これは、シグニチャが以前に作成された攻撃のみを検出できるシグニチャベースのシステムとは対照的です。
攻撃トラフィックとは何かを判断するには、システムに通常のシステムアクティビティを認識するように教える必要があります。
これはいくつかの方法で達成できますが、ほとんどの場合、人工知能タイプの手法を使用します。ニューラルネットワークを使用したシステムが使用されていますするシステムは、大きな効果を発揮するために使用されてきました。もう1つの方法は、厳密な数学的モデルを使用してシステムの通常の使用法を定義し、これからの逸脱を攻撃としてフラグを立てることです。これは、厳密な異常検出として知られています。
異常ベースの侵入検知には、いくつかの欠点があります。つまり、高い偽陽性率と、正しく配信された攻撃にだまされる可能性です。
偽陽性率が高い原因は、ユーザーとシステムの動作の通常のパターンが大きく異なる可能性があることです。

さまざまな人々がさまざまな方法で物事を行います。これらはIDSに対して 異常」として表示され、誤検知を生成する可能性があります。
不正解：
A：異常検出DSが、すでに知っている攻撃しか正しく識別できないというのは事実ではありません。
このステートメントは、署名ベースのIDSについて説明しています。
B：異常検出DSがアプリケーションベースであり、攻撃を受けやすいというのは事実ではありません。それらはハードウェアベースにすることができます。さらに、ハッカーはコンピュータシステムを攻撃します。IDSを攻撃しません。
C：異常検出DSが異常な動作を識別できないというのは真実ではありません。それはまさに彼らがしていることです。
参照：
https://en.wikipedia.org/wiki/Anomaly-based_intrusion_detection_system

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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**
仮想プライベートネットワークの作成に今日使用される可能性が低いのは次のうちどれですか？
A. L2TP
B. PPTP
C. IPSec
D. L2F
Answer: D (メーッセージを残す**)**
L2F（レイヤー2転送）は、認証または暗号化を提供しません。これは、インターネットを介した安全な仮想プライベートダイヤルアップネットワークの作成をサポートするプロトコルです。
ある時点で、L2FはPPTPとマージされ、ネットワークだけでなくネットワークで使用されるL2TPを生成しました。
リンクをダイヤルアップします。
現在、IPSecはIP環境に最適なVPNソリューションと見なされています。
出典 :HARRIS、ション、オールインワンCISSP認定試験ガイド、McGraw-Hill / Osborne、2002年、第8章：暗号化507ページ）。

最新問題**: 93**
自動ロック付きの有人施設の出入り口はどのように構成する必要がありますか？

A. フェイルセキュアになるように構成する必要があります。
B. フェイルセーフになるように構成する必要があります。
C. ドア遅延暗号ロックが必要です。
D. ピギーバックを許可しないでください。
Answer: B (メーッセージを残す**)**
アクセス制御は、施設やコンピューター、そして人々を保護することを目的としています。
状況によっては、物理的なアクセス制御と人々の生命の保護の目的
衝突する可能性があります。これらの状況では、人の人生が常に優先されます。
多くの物理的セキュリティ管理により、施設への出入りが不可能ではないにしても困難になっています。
ただし、これが生活に影響を与える可能性がある場合は、特別な配慮が必要です。情報で
処理機能では、さまざまなタイプのロックを使用でき、ピギーバックを防止する必要がありますが、
ここでの自動ロックの問題は、フェイルセーフまたはフェイルセーフとして構成できることです。
情報処理施設へのアクセスドアは1つしかないため、自動
人が操作する部屋への唯一のドアへのロックは、次の場合に人々が外に出られるように構成する必要があります
緊急事態、したがってフェイルセーフ（フェイルオープンと呼ばれることもあります）、つまり火災警報時に
起動または停電の場合、ロック装置のロックが解除されます。これは、ソレノイドが
ロックをロック状態に保つためにロックへの電力を維持することは失敗し、したがって、
電子ロック。
FailSecureは逆の方法で機能します。ロック装置は、電源が入っていない状態でロックまたは安全な状態にあります
適用。許可されたエントリで、ソリノイドは一時的にロックを解除します。したがって、Fail Secureロックでは、
火災警報器の作動力が失われると、ロックはセキュアモードのままになります。
この質問に使用される参照：
ハリス、ション（2012-10-18）。CISSPオールインワン試験ガイド、第6版（p.451）。マグロウヒル。キンドル版。
と
Hernandez CISSP、Steven（2012-12-21）。CISSP CBK、第3版の公式（ISC）2ガイド（ISC）2 Press）Kindle Locations 20249-20251）。AuerbachPublications。キンドル版。

最新問題: **94**
定義比較的少量（プライマリと比較した場合）
メモリ）非常に高速なRAMで、命令と
存在する可能性が高いプライマリメモリからのデータ

プログラムの現在実行中の部分でアクセスされるとは、
コンピュータメモリのどのカテゴリですか？
A. セカンダリ
B. 仮想
C. リアル
D. キャッシュ
Answer: (解答を表示する**)**
キャッシュロジックは、どの命令とデータを予測しようとします
メイン（プライマリ）メモリは、現在実行中のメモリによって使用されます
プログラム。次に、これらのアイテムをでより高速なキャッシュに移動します
これらのプログラムとデータを必要とするCPUの予測。ちゃんと
設計されたキャッシュは、見かけのメインメモリを大幅に削減できます
アクセス時間、したがってプログラム実行の速度を向上させます。
*回答のセカンダリメモリは低速のメモリです（磁気など
ディスク）不揮発性ストレージを提供します。
*実メモリまたはプライマリメモリはCPUによって直接アドレス指定可能であり、実行中のプログラムに関連する命令とデータの保存に使用されます。このメモリは通常、高速のランダムアクセスです
メモリ（RAM）。
*回答仮想メモリはセカンダリメモリを使用します
プライマリメモリと組み合わせて、CPUに
実際のメモリ位置のより大きく、見かけのアドレス空間。

最新問題: **95**
フォレストグリーンブックを説明する選択肢はどれですか？
A. の安全な取り扱いを定義したRainbowシリーズの本です
記憶媒体。
B. アクセス制御リストを実装するためのガイドラインを定義するRainbowシリーズの本です。
C. 存在しません。森のグリーンブックはありません。
D. ベンダーが認証者のデータ収集を支援するツールです。
Answer: A (メーッセージを残す**)**
フォレストグリーンの本は、レインボーシリーズの本で、
機密性の高いまたは分類された自動化情報システムメモリと、デガウサー、磁気テープ、ハードディスク、フロッピーディスク、カードなどのセカンダリストレージメディアの安全な処理。フォレストグリーンブックには、クリア、パージ、分類解除、または破棄の手順が詳しく説明されています
データを防ぐための自動化情報システム（AIS）ストレージメディア
残留磁気。データの残留性は、
何らかの方法で消去されたデータ。記憶媒体が消去された後
データの再構築を可能にするいくつかの物理的特性がある場合があります。

*回答 「これは、認証者のデータ収集においてベンダーを支援するツールです。」ブルーブックです、
NCSC-TG-019信頼できる製品評価アンケートバージョン2。ブルーブックは、システム開発者とベンダーが信頼できるコンピューターシステムを評価する評価者と認証者を支援するためのデータを収集するのを支援するツールです。
*回答 「アクセス制御リストを実装するためのガイドラインを定義するRainbowシリーズの本です。」グレイ/シルバーブック、NCSC-TG-020A、Trusted
UNIXワーキンググループ（TRUSIX）アクセス制御を選択する理由。
グレイ/シルバーの本は、実装のためのガイドラインを定義しています
UNIXシステムのアクセス制御リスト（ACL）。出典：NCSC-TG-
025自動化された情報におけるデータの残留性を理解するためのガイド
システム、NCSC-TG-020A信頼できるUNIXワーキンググループ
（TRUSIX）アクセス制御を選択する理由、およびNCSC-TG-019
信頼できる製品評価アンケートバージョン2。

最新問題: **96**
コントロールは、機密情報にアクセスしている個人に説明責任を提供します。この説明責任は達成されます：
A. 識別と認証を必要とするアクセス制御メカニズムと監査機能を介して。
B. システムへのアクセスの制限と情報の保護を含む論理的または技術的な制御を通じて。
C. 論理的または技術的な制御を介しますが、システムへのアクセスの制限や情報の保護は含まれません。
D. 識別と認証を必要とせず、監査機能を介して動作しないアクセス制御メカニズムを介して。
Answer: (解答を表示する**)**
コントロールは、機密情報にアクセスしている個人に説明責任を提供します。この説明責任は、識別と認証を必要とするアクセス制御メカニズムと監査機能によって実現されます。これらの管理は、組織のセキュリティポリシーに準拠し、正確に表す必要があります。保証手順により、制御メカニズムが情報システムのライフサイクル全体のセキュリティポリシーを正しく実装することが保証されます。出典：KRUTZ、Ronald L. &VINES、Russel D.、CISSP Prep Guide：Mastering the Ten Domains of Computer Security、2001、John Wiley＆Sons、33ページ

最新問題: **97**
攻撃者は、セッション状態をCookieに保存するWebアプリケーションのどのコンポーネントをバイパスできますか？
A. 認証チェック
B. 初期化チェック
C. 認証チェック
D. 本人確認
Answer: C (メーッセージを残す**)**

最新問題: **98**
認証に関して最も重要なアクションは次のうちどれですか？
A. 執行権限の取得
B. アクセス権の付与
C. 監査統制の確立
D. システムに登録しています
Answer: D (メーッセージを残す**)**

最新問題: **99**
強制アクセス制御では、オブジェクトに添付された機密ラベルにはどのような情報が含まれていますか？
A. アイテムの分類
B. アイテムの分類とカテゴリセット
C. アイテムのカテゴリ
D. アイテムの知っておくべきこと
Answer: B (メーッセージを残す**)**
以下は正しいです
アイテムの分類とカテゴリセット。
感度ラベルには、少なくとも1つの分類と1つのカテゴリセットが含まれている必要があります。
カテゴリセットとコンパートメントセットは同義語であり、同じ意味です。感度ラベル
少なくとも1つの分類と少なくとも1つのカテゴリが含まれている必要があります。一部では一般的です
単一のアイテムが複数のカテゴリに属するための環境。にすべてのカテゴリのリスト
アイテムが属するものは、コンパートメントセットまたはカテゴリセットと呼ばれます。
次の答えは正しくありません。
アイテムの分類。カテゴリセットも必要なため、正しくありません。
アイテムのカテゴリ。カテゴリセットと分類の両方が
必要。
アイテムを知る必要があります。そのようなことはないので間違っています。知る必要があるのはオブジェクトが属するカテゴリによって示されます。これは最良の答えではありません。
この質問に使用される参照：
OIG CBK、アクセス制御（186～188ページ）
AIO、第3版、アクセス制御（162～163ページ）
AIO、第4版、アクセス制御、pp212-214
ウィキペディア-http://en.wikipedia.org/wiki/Mandatory_Access_Control

最新問題: **100**
システム内のサブジェクトとオブジェクトの整合性のための正式なセキュリティモデルとして定義できるものは何ですか？

A. ビバ
B. ベルラパデュララティス
C. ラティス
D. 情報フロー
Answer: A (メーッセージを残す**)**
情報システム管理ハンドブック、1999年版、ISBN :0849399742は、次の定義を示しています。ベルラパドゥラモデルの2つの特性を研究する際に、ビバは、不正な変更の防止として定義した、もっともらしい完全性の概念を発見しました。結果として得られるBiba整合性モデルは、整合性を維持するには、データが特定の整合性のレセプタクルからより高い整合性のレセプタクルに流れないようにする必要があると述べています。たとえば、プロセスがセキュリティレベルを超えて書き込むことができる場合、信頼できるデータは、信頼性の低いデータの追加によって汚染される可能性があります。http://www.sans.org/newlook/resources/glossary.htmのSANS用語集では、次のように定義しています。システム内のサブジェクトとオブジェクトの整合性のための正式なセキュリティモデル。

最新問題**: 101**
の共同パートナーシップを確立する組織
コンピュータインシデント対応、セキュリティおよび法執行の専門家
コンピュータのセキュリティインシデントを処理し、
予防的および事後対応の両方のセキュリティサービスを提供する
A. 連邦CIO評議会
B. FederalComputerインシデントレスポンスセンター
C. CERT / CC
D. インフラストラクチャ保護センター
Answer: (解答を表示する**)**
FedCIRC憲章を再度引用すると、FedCIRCはインシデント対応の支援とガイダンスを提供し、機関の境界を越えたインシデント処理への集中型アプローチを提供します。具体的には、FedCIRCの使命は次のとおりです。民間機関に技術情報、ツール、方法、支援、およびガイダンスを提供する積極的であり、連絡活動と分析サポートを提供する連邦政府機関との協力関係を通じて高品質の製品とサービスの開発を奨励する防衛省、学界、および民間企業政府情報技術（IT）リソースの最高のセキュリティプロファイルを促進する連邦政府とのインシデント対応および手続き上の認識の処理を促進する
* Answer CERT Coordination Center（CERT / CC）は、カーネギーメロン大学ソフトウェアエンジニアリングインスティテュート（SEI）のユニットです。SEIは、連邦政府が資金提供するR＆Dセンターです。CERTの使命は、インターネットコミュニティに脆弱性と攻撃を警告し、インシデント対応を含むコンピュータセキュリティの分野で調査とトレーニングを実施することです。
*回答「インフラストラクチャ保護センター」は気を散らすものであり、連邦最高情報責任者評議会である「連邦CIO評議会」はFedCIRCのスポンサーです。

最新問題**: 102**

懲役は以下の判決の可能性があります：
A. 民法でも刑法でもない
B. 民法と刑法の両方
C. 民事（不法行為）法
D. 刑法
Answer: (解答を表示する**)**
正解は刑法です。それは投獄が可能な唯一の選択肢です。

最新問題: **103**
サービス拒否（DoS）攻撃から保護するためのコントロールは、攻撃の50%を阻止し、さらに攻撃の影響を50%削減することが決定されています。残存リスクとは何ですか？
A. 100%
B. 25%
C. 75%
D. 50%
Answer: B (メーッセージを残す**)**

最新問題: **104**
クリアテキストパスワード、チャレンジレスポンス、任意のダイアログシーケンスなど、PPPの複数のオプションの認証メカニズムをサポートするフレームワークとして定義できるのは次のうちどれですか？
A. 拡張認証プロトコル
B. チャレンジハンドシェイク認証プロトコル
C. リモート認証ダイヤルインユーザーサービス
D. マルチレベル認証プロトコル。
Answer: A (メーッセージを残す**)**
RFC 2828（Internet Security Glossary）は、Extensible Authentication Protocolを、クリアテキストパスワード、チャレンジレスポンス、任意のダイアログシーケンスなど、PPPの複数のオプションの認証メカニズムをサポートするフレームワークとして定義しています。これは主に、交換回線またはダイヤルアップ回線を介してPPPネットワークサーバーに接続するホストまたはルーターによる使用を目的としています。リモート認証ダイヤルインユーザーサービス（RADIUS）は、共有の集中認証サーバーと、ネットワークアクセスのユーザーを認証する必要があるネットワークアクセスサーバーとの間で、ダイヤルインユーザーの認証情報と構成情報を伝送するためのインターネットプロトコルとして定義されます。ポート。他のオプションは気を散らすものです。出典：SHIREY、Robert W.、RFC2828：Internet Security Glossary、2000年5月

最新問題: **105**
束ねられたケーブル配線に関連するどの無線周波数干渉（RFI）現象が、情報漏えいを引き起こす可能性がありますか？
A. 出血

B. 転移
C. 被覆通信路
D. クロストーク
Answer: D (メーッセージを残す**)**

最新問題**: 106**
認証プロセスの主な結果は、文書化されたものを提供することです
A. 修復のためのシステムの弱点。
B. セキュリティ評価、テスト、およびプロセス評価の基準。
C. 相互接続されたシステムとそれらに実装されたセキュリティ制御。
D. リスクベースの意思決定を行うために必要なセキュリティ分析。
Answer: D (メーッセージを残す**)**

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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**
次のうち、ハードウェア保持ポリシーを含める必要があるのはどれですか？
A. データを1週間だけ保持し、保持をサードパーティベンダーにアウトソーシングする
B. 保持する前に機密データを暗号化するための暗号化テクノロジーの使用
C. ビジネス目的でのみ必要な日付と保持スケジュールを保持する計画
D. メディアとハードウェア上のすべての機密データの保持
Answer: (解答を表示する**)**

最新問題**: 108**
ある組織が、ユーザーが匿名プロキシを使用して許可されていないWebサイトにアクセスしていることを発見しました。
次のうちどれが将来の発生を防ぐための最良の方法ですか？
A. プロキシ要求のインターネットプロトコル（IP）トラフィックを分析します
B. 既知の匿名プロキシのインターネットプロトコル（IP）アドレスをブロックする
C. プロキシから匿名性を削除します
D. ファイアウォールのプロキシサーバーを無効にします
Answer: D (メーッセージを残す**)**

最新問題**: 109**

次のリスク分析用語のどれが、リスクを低減するセーフガードの欠如または弱点を特徴づけますか？
A. 脅威
B. 確率
C. 脆弱性
D. 期待損失
Answer: C (メーッセージを残す**)**
システムセキュリティ手順、システム設計、実装、内部制御などの弱点が悪用されて、システムセキュリティポリシーに違反する可能性があります。-Ronald Krutz CISSP PREPガイド ゴールドエディション）927ページ

最新問題**: 110**
十分な注意は以下とは関係ありません。
A. 誠意を持って
B. 賢い人
C. 利益
D. 最大の関心事
Answer: C (メーッセージを残す**)**
会社の役員および取締役は、その任務を遂行する上で慎重に行動することが期待されています。取締役は誠意を持って行動し、同様の立場にある通常の賢明な人物が同様の状況下で、企業の最善の利益になると合理的に信じる方法で行使するように注意します。利益の概念は、適切なケアの原則に反する傾向があります。出典 :ANDRESS、Mandy、Exam Cram CISSP、Coriolis、2001年、第10章：法律 調査、および倫理 （186ページ）。

最新問題**: 111**
以下の選択は、結果として生じる潜在的な危険とは見なされません
自然の出来事から？
A. 山火事
B. 都市火災
C. アーソン
D. 地震/土地シフト
Answer: C (メーッセージを残す**)**
NFPAによると、放火は潜在的な危険の例です
人間の出来事によって引き起こされます。火自体は、考慮されます
放火が炎の原因であると考えられていない限り、森林火災、範囲火災、都市または都市の火災などの自然の出来事。潜在的な危険の3つのカテゴリー（自然 技術、および人間）のうち、人間のイベントには次のものが含まれる可能性があります。
ゼネスト
テロ
サボタージュ

集団ヒステリー
市民の不安
出典：災害緊急事態管理に関するNFPA1600標準
and Business Continuity、全米防火協会、2000年
版。

最新問題: **112**
以下にリストされている構成管理のどの要素に、
構成アイテム（CI）の使用？
A. 構成の識別
B. 構成制御
C. 構成監査
D. 構成会計
Answer: A (メーッセージを残す**)**
構成管理には、検証の分解が伴います
システムを識別可能、理解可能、管理可能、追跡可能に
構成アイテム（CI）と呼ばれるユニット。CIは独自のものです
最小部分を表すシステムの識別可能なサブセット
独立した構成管理手順の対象となります。The
検証システムのCIへの分解プロセスはと呼ばれます
構成の識別。CIは、サイズ、タイプ、および
複雑。のための厳格なルールはありませんが
分解、CIの粒度は非常に実用的です
重要性。有利な戦略は、比較的大きなCIを指定することです
の寿命にわたって変化することが期待されていない要素の場合
システム、およびより頻繁に変更される可能性のある要素の小さなCI。
* 「構成アカウンティング」（構成アカウンティング）に回答すると、構成制御アクティビティのステータスが文書化され、一般に情報が提供されます。
構成を効果的に管理するために必要です。それはマネージャーがすることを可能にします
システムの変更を追跡し、開発の履歴を確立します
問題と関連する修正。
回答「構成監査」、構成監査は、構成管理の品質保証コンポーネントです。これには、アカウンティング情報の一貫性と完全性を判断し、すべての構成管理ポリシーが遵守されていることを確認するための定期的なチェックが含まれます。
回答「構成制御」、構成制御は、システム変更が実装される前に承認され、提案および承認された変更のみが実装され、実装が
完全で正確。
出典：NCSC-TG-014-89、フォーマル検証システムのガイドライン。

最新問題: **113**
侵入者を首尾よく起訴できるようにするために：
A. 法執行機関やその他の外部機関との連絡を担当する連絡先を指定する必要があります。
B. 証拠の適切な管理過程を維持する必要があります。
C. 証拠の収集は、事前定義された手順に従って行う必要があります。
D. 可能な限り、元のリソースではなく、侵害されたリソースのレプリカを分析して、不注意に証拠を突き刺さないようにします。
Answer: B (メーッセージを残す**)**
説明/参照：
Explanation:
証拠が押収された場合、刑事訴訟や起訴の成功などの後の出来事に使用する必要がある場合に備えて、収集されたデータを後で適切かつ正確に表すことができるように、適切な管理過程が維持されていることを確認することが重要です。
不正解：
A：侵入者を首尾よく起訴するために、設計された連絡先は必要ありません。証拠の適切な管理過程が必要です。
C：侵入者を首尾よく起訴するには、事前定義された手順に従わないでください。証拠の適切な管理過程が必要です。
D：起訴を成功させるために厳密に要求されているわけではありませんが、証拠との衝突を避けるためにデジタル証拠のレプリカを作成することは重要です。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、New York、2013、p。248

最新問題: **114**
プロセッサカードには、次のコンポーネントのどれが含まれていますか？
A. メモリとハードドライブ。
B. メモリとフラッシュ。
C. メモリとプロセッサ。
D. キャッシュとプロセッサ。
Answer: C (メーッセージを残す**)**
プロセッサカードには、メモリとプロセッサが含まれています。それらは驚くべきデータ処理能力を持っています。多くの場合、データ処理能力はデータの暗号化/復号化に使用されるため、このタイプのカードは非常にユニークな個人識別トークンになります。データ処理により、動的なストレージ管理も可能になり、柔軟な多機能カードの実現が可能になります。

最新問題: **115**
キーの選択とデータの暗号化に関連する計算は複雑であり、手動での使用には実用的ではありません。ただし、モジュラー演算の数学的特性と「_____」として知られる方法を使用すると、RSAはコンピューターでの使用に非常に適しています。

A. ガロア体での計算
B. グラッデンフィールドでの計算
C. ガリポリフィールドでのコンピューティング
D. ガルブレイスフィールドでの計算
Answer: A (メーッセージを残す**)**
キーの選択とデータの暗号化に関連する計算は複雑であり、手動での使用には実用的ではありません。ただし、モジュラー演算の数学的特性とガロア体での計算として知られる方法を使用すると、RSAはコンピューターでの使用に非常に適しています。出典：FITES、Philip E.、KRATZ、Martin P.、Information Systems Security：A Practitioner's Reference、1993、Van Nostrand Reinhold、44ページ。

最新問題**: 116**
ユーザーIDの信頼できるソースとしてIdentityasa Service（IDaaS）と統合するために、クラウドサービスまたはオンプレミスを介して展開できるサービスは次のうちどれですか？
A. ユーザーデータベース
B. シングルサインオン（SSO）
C. 多要素認証（MFA）
D. ディレクトリ
Answer: D (メーッセージを残す**)**

最新問題**: 117**
次のうち、OSIによって定義された基本的なセキュリティサービスではないものはどれですか？
A. ルーティング制御
B. 認証
C. データの機密性
D. ロギングとモニタリング
Answer: (解答を表示する**)**
ルーティング制御は定義されていますが、ロギングとモニタリングについては言及されていません。参照：
http://en.wikipedia.org/wiki/Security_service_(telecommunication）
と
http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.800-199103-I!!PDF-E&type=items

最新問題**: 118**
企業はハードドライブの再利用プログラムに登録されており、廃止された機器は不要になったときにベンダーに売り戻されます。ベンダーは、機能しなくなった機器よりも機能しているドライブに多くのお金を支払います。ベンダーから最も多くのお金を受け取りながら、不正なデータの損失を防ぐ最も安全な手段を提供するデータサニタイズの方法はどれですか？
A. マルチパスワイプ
B. シングルパスワイプ

C. 消磁
D. ピン留め
Answer: C (メーッセージを残す**)**

最新問題**: 119**
6階建てのビルに情報処理施設を配置するのに最適なフロアは次のうちどれですか。
A. 地下
B. 1階
C. 3階
D. 6階
Answer: C (メーッセージを残す**)**
データセンターは、自然災害や爆弾からの保護を提供し、必要に応じて緊急時の乗組員が簡単にアクセスできるように、施設の中央または建物の中心部に配置する必要があります。施設の中核となることにより、外壁は保護の二次層としても機能します。
屋上から火災や洪水が発生した場合に備えて、情報処理施設を建物の最上階に配置しないでください。屋根に大きな穴を開けるだけで、多くの犯罪や盗難が発生しています。
水が自然に流れ落ちる傾向がある洪水のため、地下室に置くべきではありません:-)少しの水でも、レイズフロアの下のセメントフロアに直接座っている電気ケーブルの量を考えると、操作に影響します。
人々が出入りする正面玄関があるため、データセンターを1階に配置しないでください。エレベーター、船積みドック、カフェテリア、コーヒーショップなど、交通量の多いエリアがたくさんあります。データセンターとしては本当に悪い場所です。
そのため、上部、下部、地下室がすべて悪い選択である除去プロセスを使用することで、答えを簡単に思い付くことができました。それはあなたに3階である唯一の可能な答えを残しました。
出典 :ハリス、ション、オールインワンCISSP認定試験ガイド、第5版、ページ
425。

最新問題**: 120**
アクセス制御のセキュリティ評価を実施する場合、データ分析フェーズの一部となるアクティビティはどれですか。
A. 監査中に収集された証拠を分類して特定します。
B. データトランザクションの統計的サンプリングを実施します。
C. ログとレポートを収集します。
D. 監査の例外に対処するためのソリューションを提示します。
Answer: A (メーッセージを残す**)**

最新問題**: 121**
次のうち、モーションディテクタのタイプではないものはどれですか？
A. 光電センサー
B. パッシブ赤外線センサー

C. マイクロ波センサー。
D. 超音波センサー。
Answer: (解答を表示する**)**
説明/参照：
Explanation:
光電センサーは動きを検出しません。光のビームの途切れを検出します。
光電システム、または測光システムは、光ビームの変化を検出します。これらのシステムは、受信機に当たるビームを放出する光電式煙探知器のように機能します。この光線が遮られると、アラームが鳴ります。光電セルによって放出されるビームは、断面であり得、不可視または可視ビームであり得る。断面とは、1つの領域に複数の異なる光ビームが広がる可能性があることを意味します。これは通常、隠しミラーを使用して、光レシーバーに当たるまでビームをある場所から別の場所にバウンスすることによって実行されます。
不正解：
B：パッシブ赤外線システム（PIR）は、監視するように構成されている領域の熱波の変化を識別します。空気中の粒子の温度が上昇した場合、侵入者の存在を示している可能性があるため、アラームが鳴ります。PIRはモーションディテクタの一種です。したがって、この答えは正しくありません。
C：波パターンモーションディテクタは、監視する波の周波数が異なります。異なる周波数は、マイクロ波、超音波、および低周波数です。これらのデバイスはすべて、敏感な領域を介して送信され、受信機に反射される波形パターンを生成します。パターンが邪魔されずに返される場合、デバイスは何もしません。部屋の中の何かが動いているためにパターンが変更されて戻った場合、アラームが鳴ります。マイクロ波センサーは、モーションディテクターの一種です。したがって、この答えは正しくありません。
D：超音波センサーは波パターンモーションディテクターの一例です。したがって、この答えは正しくありません。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、2013、p。495

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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**
次のうち、探偵の技術的管理の形式ではないものはどれですか？
A. 取引の履歴
B. アクセス制御ソフトウェア

C. ハニーポット
D. 侵入検知システム
Answer: B (メーッセージを残す**)**
探偵の技術的管理は、技術的アクセス管理違反を警告します。
アクセス制御ソフトウェアは、予防的な技術的制御の一例です。他の選択肢は、探偵の技術的管理を表しています。
出典 :DUPUIS、Cl？ment、アクセス制御システムおよび方法論CISSP Open Study ガイド、バージョン10 (2002年3月)。

最新問題**: 123**
DESキーは次のとおりです。
A. 56ビット。
B. 512ビット。
C. 64ビット。
D. 128ビット。
Answer: (解答を表示する**)**

最新問題**: 124**
構造化照会言語のリテラル値のプレースホルダーは次のうちどれですか
(SQL)クエリがサーバー上のデータベースに送信されていますか？
A. 変数をバインドする
B. 同化変数
C. 削減変数
D. 解像度変数
Answer: (解答を表示する**)**
バインド変数は、構造化クエリのリテラル値のプレースホルダーです
サーバー上のデータベースに送信される言語 (SQL)クエリ。
出典 :KRUTZ、Ronald L. &VINES、Russel D.、CISSP準備ガイド :マスタリング コンピュータセキュリティの10のドメイン、2001年、John Wiley&Sons、47ページ。

最新問題**: 125**
次のうち、生体認証を扱う際のリプレイ攻撃を一般的に示しているのはどれですか？
A. 本人拒否率 (FRR)が100分の5より大きい
B. 他人受入率 (FAR)が100,000人に1人を超える
C. 完全一致
D. 不適切に指定されたテンプレート
Answer: C (メーッセージを残す**)**

最新問題**: 126**

参照整合性では、外部キー属性について、参照されるリレーションに同じ値のタプルが必要です。次のうちどれですか。

A. 主キー

B. 二次キー

C. 外部キー

D. 候補キー

Answer: (解答を表示する**)**

説明/参照：

Explanation:

外部キーは、あるテーブルの属性であり、別のテーブルの主キーを参照または一致します。主キーは、テーブル内の各行またはタプルが一意であることを確認するために使用される属性です。一緒に、外部キーと主キーは参照整合性を保証します。

不正解：

B：セカンダリキーは、プライマリキーとして選択されていない候補キーです。主キーは、テーブル内の各行またはタプルを一意にするために使用される属性です。候補キーは、データベース開発者が主キーを選択できる属性のサブセットです。

C：外部キーは、あるテーブルの属性であり、別のテーブルの主キーと一致し、テーブルを相互参照するために使用されます。

D：候補キーは属性のサブセットであり、データベース開発者はそこから主キーを選択して、テーブル内のタプルまたはレコードを一意に識別できます。

参照：

Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、New York、2013、pp.1174、1179-1180、1181

Stewart、James、Ed Tittel、Mike Chapple、CISSP：Certified Information Systems security Professional Study Guide、第5版、Wiley Publishing、インディアナポリス、2011年、276、312ページ

http://databases.about.com/cs/specificproducts/g/candidate.htm

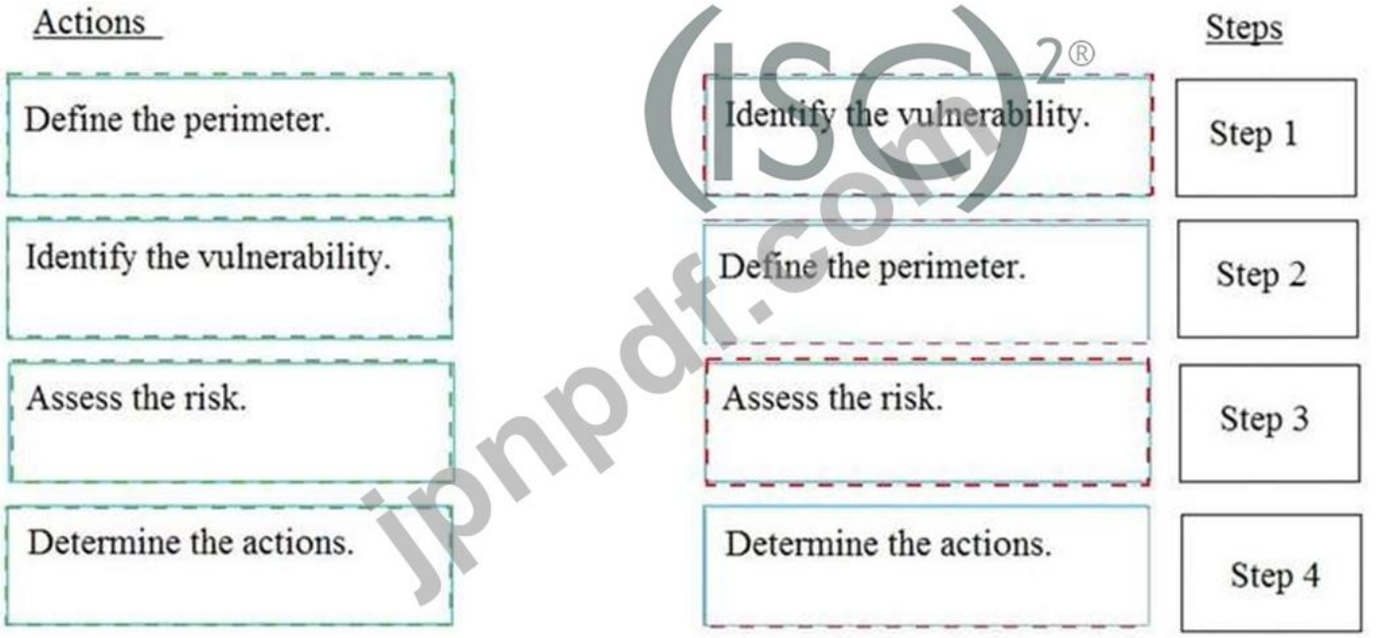
http://rdbms.opengrass.net/2_Database Design / 2.1_TermsOfReference / 2.1.2_Keys.html

最新問題**: 127**

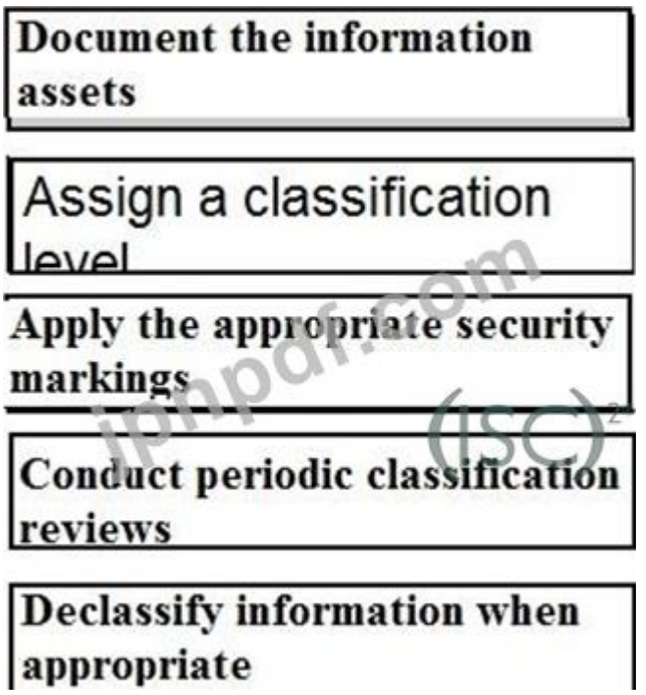
次の情報分類手順を順番に並べます。

Steps
Order
Declassify information when appropriate
Apply the appropriate security markings
Conduct periodic classification reviews
Assign a classification level
Document the information assets
Step
Step
Step
Step
Step

Answer:


Actions
Define the perimeter.
Identify the vulnerability.
Assess the risk.
Determine the actions.
Steps
Identify the vulnerability.
Define the perimeter.
Assess the risk.
Determine the actions.
Step 1
Step 2
Step 3
Step 4

説明



最新問題: **128**
次のうち、Kerberosプロトコルに当てはまらないものはどれですか？
A. セッションごとに必要なログインは1回だけです。
B. 最初の認証手順は、公開鍵アルゴリズムを使用して行われます。
C. KDCはネットワーク内のすべてのシステムを認識しており、それらすべてから信頼されています
D. 相互認証を行います
Answer: B (メーッセージを残す**)**
Kerberosはネットワーク認証プロトコルです。これは、秘密鍵暗号化を使用して、クライアント/サーバーアプリケーションに強力な認証を提供するように設計されています。次の特徴があります。
*安全です。暗号化されていない限り、パスワードを送信することはありません。
*セッションごとに1回のログインのみが必要です。ログイン時に定義された資格情報は、追加のログインを必要とせずにリソース間で渡されます。
*概念は、信頼できるサードパーティであるキー配布センター（KDC）に依存します。The KDCはネットワーク内のすべてのシステムを認識しており、それらすべてから信頼されています。
*相互認証を実行します。この場合、クライアントはサーバーに対してIDを証明し、サーバーはクライアントに対してIDを証明します。
Kerberosは、チケット許可サーバー/サービス（TGS）の概念を導入しています。サービスの使用を希望するクライアントは、TGSからチケットを受信する必要があります（チケットは時間制限のある暗号化メッセージです）。サーバーへのアクセスを許可します。Kerberosには、クライアントを検証するための認証サーバー（AS）。2つのサーバーを組み合わせてKDCを構成します。

Windows環境内で、ActiveDirectoryはKDCの機能を実行します。次の図は、クライアントがKerberos認証を使用してサービスにアクセスするために必要な一連のイベントを示しています。各ステップは、RFC 4120 「Kerberosネットワーク認証サービス」で定義されているように、関連付けられたKerberosメッセージとともに示されます。
「V5）」。
ステップバイステップのKerberos認証
*ステップ1 :ユーザーはワークステーションにログオンし、ホストでサービスを要求します。ワークステーションは、チケット許可チケットを要求するメッセージを承認サーバーに送信します（ターゲット）。
*ステップ2：認証サーバーは、ユーザーデータベースでのユーザーのアクセス権を確認し、TGTとセッションキーを作成します。Authorization Severは、ユーザーのパスワードから取得したキーを使用して結果を暗号化し、ユーザーのワークステーションにメッセージを送り返します。
ワークステーションはユーザーにパスワードの入力を求め、そのパスワードを使用して着信メッセージを復号化します。復号化が成功すると、ユーザーはTGTを使用してサービスチケットを要求できるようになります。
*ステップ3 :ユーザーがサービスへのアクセスを希望する場合、ワークステーションクライアントアプリケーションは、クライアント名、レルム名、およびタイムスタンプを含む要求をチケット付与サービスに送信します。ユーザーは、ステップ2で受信したセッションキーで暗号化されたオーセンティケーターを送信することにより、自分のIDを証明します。
*ステップ4 :TGSはチケットとオーセンティケーターを復号化し、要求を検証して、要求されたサーバーのチケットを作成します。チケットにはクライアント名とオプションでクライアントが含まれています
IPアドレス。また、レルム名とチケットの有効期間も含まれています。TGSは、チケットをユーザーワークステーションに返します。返されたメッセージには、サーバーセッションキーの2つのコピーが含まれています
-1つはクライアントパスワードで暗号化され、もう1つはサービスパスワードで暗号化されています。
*ステップ5 :クライアントアプリケーションは、ステップ4で受信したチケットとオーセンティケーターを含むサービスリクエストをサーバーに送信するようになりました。サービスは、セッションキーを復号化することによって要求を認証します。サーバーは、チケットとオーセンティケーターが一致することを確認してから、サービスへのアクセスを許可します。説明するこの手順には、後で説明するIntelAMTデバイスによって実行される認証は含まれません。
*ステップ6：相互認証が必要な場合、サーバーはサーバー認証メッセージで応答します。
Kerberosサーバーは、その制御下にあるすべてのクライアントとサーバーの「シークレット」（暗号化されたパスワード）を認識しているか、この情報を持つ他の安全なサーバーと接続しています。これらの「秘密」は、上の図に示されているすべてのメッセージを暗号化するために使用されます。
「リプレイ攻撃」を防ぐために、Kerberosはプロトコル定義の一部としてタイムスタンプを使用します。タイムスタンプが正しく機能するためには、クライアントとサーバーのクロックが可能な

限り同期している必要があります。つまり、両方のコンピューターを同じ日時に設定する必要があります。2台のコンピューターのクロックが同期していないことが多いため、管理者は、クライアントのクロックとサーバーのクロックの間にKerberosとの最大許容差を確立するためのポリシーを確立できます。クライアントの時計とサーバーの時計の差がこのポリシーで指定されている最大時間差よりも小さい場合、2台のコンピューター間のセッションで使用されるタイムスタンプはすべて本物と見なされます。最大差は通常5分に設定されています。
クライアントアプリケーションが「Kerberized」サービスはKerberos認証を実行するように構成されている）のサービスを使用する場合、必要なメッセージ応答をサポートすることを期待できるように、クライアントもKerberizedである必要があることに注意してください。
Kerberosの詳細については、http ://web.mit.edu/kerberos/www/を参照してください。
参照：
IntelによるKerberos認証の概要
と
http://www.zeroshell.net/eng/kerberos/Kerberos-definitions/#1353
と
http://www.ietf.org/rfc/rfc4120txt

最新問題: **129**
データ分類プログラムを成功させるための重要な要素は次のうちどれですか？
A. エンドユーザーの受け入れ
B. 情報セキュリティスポンサーシップ
C. エグゼクティブスポンサー
D. 内部監査の承認
Answer: C (メーッセージを残す**)**

最新問題: **130**
脆弱性評価レポートがクライアントに提出されました。クライアントは、スコープ内にあったホストの3分の1がレポートから欠落していることを示します。
このエラーは、評価のどのフェーズで発生した可能性が最も高いですか？
A. 列挙
B. レポート
C. 検出
D. 発見
Answer: (解答を表示する**)**
セクション :セキュリティの評価とテスト

最新問題: **131**
次のタイプのセキュリティテストのうち、セキュリティリスク評価を実行するときに組織の日常のセキュリティ課題をより適切に示すのに最も効果的なのはどれですか？
A. 秘密

B. 内部
C. 明白
D. 外部
Answer: (解答を表示する**)**

最新問題**: 132**
システムエンジニアリングライフサイクル（SELC）ステージ内のプロセスは次のうちどれですか？
A. 開発と展開
B. 生産業務
C. 要件分析
D. 利用サポート
Answer: C (メーッセージを残す**)**

最新問題**: 133**
ドラッグアンドドロップの質問
ハイパーテキスト転送プロトコル（HTTP）認証タイプを、相対的な強度の順に以下にランク付けします。
強度に応じて、認証タイプを右側の正しい位置にドラッグします。

Answer:

最新問題**: 134**
次のツールのうち、ハッカーが使用する可能性が低いものはどれですか？
A. l0phtcrack
B. トリップワイヤー
C. OphCrack
D. ジョン・ザ・リッパー

Answer: B (メーッセージを残す**)**
Tripwireは整合性チェック製品であり、重要なファイル（システムファイルや構成ファイルなど）が変更されたときにアラームをトリガーします。
これは、それを回避するためにその動作を研究する以外に、ハッカーによって使用される可能性が低いツールです。
他のプログラムはパスワードクラッキングプログラムであり、ハッカーだけでなくセキュリティ管理者によっても使用される可能性があります。で利用可能なTripwireに関する詳細情報
Tripwire、Inc.のWebサイト。
ノート：
Tripwireの商用バージョンの最大の競争相手は、フリーウェアバージョンです。
トリップワイヤー。次のURLでTripwireのオープンソースバージョンを入手できます。
http://sourceforge.net/projects/tripwire/

最新問題: **135**
サブジェクト名を公開鍵値にバインドするのは次のうちどれですか？
A. 公開鍵証明書
B. 公開鍵インフラストラクチャ
C. 秘密鍵インフラストラクチャ
D. 秘密鍵証明書
Answer: B (メーッセージを残す**)**
公開鍵証明書という用語は、デジタル証明書またはID証明書と同義であることに注意してください。
証明書自体がバインディングを提供しますが、実際にバインディングを検証し、証明書内のキーの所有者のIDを保証する認証局（CPS）を通過するのは認証局です。
ウィキペディアで説明されているように：
暗号化では、公開鍵証明書（デジタル証明書またはID証明書とも呼ばれます）は、デジタル署名を使用して公開鍵とIDをバインドする電子ドキュメントです。
-個人または組織の名前、住所などの情報。証明書を使用して、公開鍵が個人に属していることを確認できます。
一般的な公開鍵インフラストラクチャ（PKI）スキームでは、署名は認証局（CA）のものになります。PGPやGPGなどの信頼スキームのWebでは、署名は、ユーザー（自己署名証明書または他のユーザー（承認」）のいずれかであり、ユーザーが互いにキーに署名するようにします。いずれの場合も、証明書の署名は、ID情報と公開鍵が一緒に属していることを示す証明書署名者による証明です。RFC 2828は、認証局（CA）を次のように定義しています。
デジタル証明書（特にX.509証明書）を発行し、証明書内のデータ項目間のバインドを保証するエンティティ。
証明書を作成および割り当てるために1人以上のユーザーによって信頼される権限。オプションで、証明機関がユーザーのキーを作成する場合があります。

X509証明書のユーザーは、証明書によって提供される情報の有効性に依存します。したがって、CAは、証明書ユーザーが信頼する人物である必要があり、通常、政府、企業、またはその他の組織によって作成され、権限が付与された公式の地位を保持します。CAは、証明書のライフサイクルを管理する責任があり、証明書のタイプと適用されるCPSによっては、証明書に関連付けられたキーペアのライフサイクルを担当する場合があります。
出典 :SHIREY、Robert W.、RFC2828 :Internet Security Glossary、2000年5月。および
http://en.wikipedia.org/wiki/Public_key_certificate

最新問題**: 136**
データ所有者（ファイルを作成した人）が所有する情報へのアクセスを制御できるようにするアクセス制御方法はどれですか？
A. DAC-随意アクセス制御
B. MAC-強制アクセス制御
C. RBAC-役割ベースのアクセス制御
D. NDAC-非随意アクセス制御
Answer: A (メーッセージを残す**)**
DAC-随意アクセス制御は、ユーザーが作成または管理するデータへのアクセスを制御する場所です。
これは、いくつかの要因のために、アクセス制御の最も安全性の低い方法です。
-従業員の交代は、データの所有権の混乱やデータの放棄につながる可能性があります。
-従業員は従来、データのアクセス許可を管理し、信頼できる方法で維持するのに十分な経験がありません。
-一般的に、人は組織の中で最も信頼性の低いコンポーネントです。次の答えは正しくありません。
-MAC-強制アクセス制御 :アクセス制御のMACモデルでは、データの機密性のレベルを識別するためにラベルが使用されるため、これは正しくありません。ユーザーがそのようなデータに対する特権を持っていない場合、彼または彼女はアクセスを拒否されます。
-RBAC-役割ベースのアクセス制御：申し訳ありませんが、RBACは役割ベースのアクセス制御であり、ユーザーの役割によって、与えられたデータへのアクセスレベルが決まります。
-NDAC-非随意アクセス制御：申し訳ありませんが、これはアクセス制御方法論に関連する一般的な用語ではありません。
この質問を作成するために、次の参照が使用されました :2013公式セキュリティ+カリキュラム。

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

こちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (1533330%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
次の回答のうち、ユーザーに高可用性を提供することに直接関係しているのはどれですか？
A. バックアップデータ回路
B. 優れた雇用慣行
C. 更新されたウイルス対策ソフトウェア
D. 上級管理職サポート
Answer: A (メーッセージを残す)
説明/参照：
Explanation:
高可用性を計画する場合、データネットワークの重要なコンポーネントには、障害が発生した場合に備えて、何らかの冗長性またはバックアップ計画を立てる必要があります。
情報資産への中断のないアクセスを提供する方法の1つは、冗長性とフォールトトレランスを使用することです。冗長性とは、物理コンポーネントまたは論理コンポーネントの複数のインスタンスを提供して、最初のコンポーネントに障害が発生した場合に2番目のコンポーネントを使用できるようにすることです。フォールトトレランスは、冗長性を含むより広い概念ですが、障害が発生した場合にシステムが情報資産を引き続き利用できるようにするプロセスを指します。
これには、次のようなアイテムを含めることができます。
サーバー上のRAIDアレイディスク。これにより、単一のドライブに障害が発生した場合でも、サーバーは引き続き使用可能です。
▪
ネットワーク接続をバックアップします。多くのインターネットサービスプロバイダーは、これらを有料で提供しています。
▪
すべてのシステムと回路のバックアップ電源。
▪
消火および避難計画。
▪
オフサイトの安全なリモートにバックアップを保存しながら、データをバックアップおよび復元するためのデータバックアップの実践
▪
位置。
不正解：
B：優れた雇用慣行により、優れたスタッフを確実に採用することができます。ただし、これは高可用性を保証するものではありません。
C：更新されたウイルス対策ソフトウェアは、多層防御の重要な部分ですが、高可用性を保証しません。
D :シニアエグゼクティブサポート。これは高可用性のための機器への資金提供には重要ですが、高可用性の提供とは直接関係ありません。

最新問題: 138

ワンタイムパッドを適切に使用した場合、次のどの特性がありますか？
A. キーは、暗号化するメッセージよりも長い必要があります。
B. キーはランダムである必要はありません。
C. 複数回使用できます。
D. 壊れません。
Answer: (解答を表示する**)**
正解は「壊れない」です。ワンタイムパッドが1回だけ使用され、対応するキーが本当にランダムで、繰り返し文字がない場合、壊れることはありません。
「複数回使用できる」という回答は、使用した場合は正しくありません。
適切には、ワンタイムパッドは1回だけ使用する必要があります。
キーはランダムである必要があるため、「キーはランダムである必要はありません」という回答は正しくありません。
キーはメッセージと同じ長さである必要があるため、「キーは暗号化するメッセージよりも長い長さである必要があります」という回答は正しくありません。

最新問題**: 139**
設計者が潜在的な脆弱性の軽減戦略を開発できるようにするテスト手法は何ですか？
A. 手動検査とレビュー
B. 侵入テスト
C. 脅威モデリング
D. ソースコードレビュー
Answer: (解答を表示する**)**
https://owasp.org/www-project-web-security-testing-guide / asset / archive / OWASP_Testing_Guide_v4.pdf（15）

最新問題**: 140**
IDおよびアクセスプロビジョニングのライフサイクルの2番目のステップは何ですか？
A. プロビジョニング
B. レビュー
C. 承認
D. 失効
Answer: B (メーッセージを残す**)**
セクション：IDおよびアクセス管理（IAM）

最新問題**: 141**
次のプロトコルのうち、Webアプリケーショントラフィックに対する盗聴攻撃の脅威を最もよく軽減するのはどれですか？
A. SSLまたはTLS
B. 802.1X
C. ARPキャッシュセキュリティ

D. SSH-セキュアシェル
Answer: (解答を表示する**)**
それがネットワークを横断している間、Webアプリケーションのある種の暗号化なしで
データは、ネットワーク上の攻撃者によるスニッフィングや傍受に対して脆弱です。スニファを観察すると
暗号化されていないネットワーク上のトラフィックは、Webとのユーザーインタラクションの内容を明確に見ることができます
サーバーとそのアプリケーション。
SSL-SecureSocketsLayerまたはTLS-トランスポート層のセキュリティ
これら2つのプロトコルには類似点がありますが、TLS3.1はSSL2.0に取って代わりますが、
相互運用性はありません。現在、両方のプロトコルが多くのWebサーバーで一般的に使用されています。どちらの場合にも
SSL / TLSは、ネットワークトラフィックがワイヤを通過するときに暗号化し、盗聴攻撃から保護します。
次の答えは正しくありません。
802.1X :これは転送中のデータを保護しませんが、許可されていないデバイスが
ネットワークに接続してデータをスニッフィングします。「ドット1X」または 「エクステンシブル」とも呼ばれます
認証プロトコル（EAP）」は、証明書を要求することによってインフラストラクチャ保護を提供します
接続。
ARPキャッシュセキュリティ :これは、Webアプリデータのネットワークスニッフィングの脅威を軽減しません。
SSH-セキュアシェル：不正解です。SSHは、トラフィックを暗号化して軽減するTELNETの代替品です。
SSH接続でのネットワークスニファの脅威。
この質問を作成するために、次の参照が使用されました。
2011. EC-COUNCIL公式カリキュラム、倫理的ハッキングと対策、v7.1、モジュール13
ページ569。

最新問題**: 142**
接触型と非接触型の両方の形式を利用できる2つのチップを備えたスマートカードは、次のように呼ばれます。
A. スマートカードに連絡する
B. 非接触型スマートカード
C. ハイブリッドカード
D. コンビカード
Answer: C (メーッセージを残す**)**

これは、非接触形式と非接触形式の両方を利用できる2つのチップを備えた非接触型スマートカードです。カードの2つの追加カテゴリは、上記のデュアルインターフェイスカードとハイブリッドカードです。ハイブリッドカードハイブリッドカードには2つのチップがあり、1つは接触型インターフェースを備え、もう1つは非接触型インターフェースを備えています。2つのチップは相互接続されていません。
デュアルインターフェイスカードこのカードをハイブリッドカードと混同しないでください。これはチップが1つだけです。デュアルインターフェイスカードには、接触インターフェイスと非接触インターフェイスの両方を備えたシングルチップが搭載されています。デュアルインターフェイスカードを使用すると、非常に高いレベルのセキュリティを備えた接触型または非接触型インターフェイスを使用して同じチップにアクセスできます。
カードの内部動作これらのカードすべてで使用されるチップは、マイクロコントローラチップとメモリチップの2つのカテゴリにも分類されます。メモリチップは、オプションのセキュリティを備えた小さなフロッピーディスクのようなものです。メモリチップはマイクロコントローラよりも安価ですが、それに応じてデータ管理のセキュリティが低下します。メモリチップを使用するカードは、処理するカードリーダーのセキュリティに依存しており、低または中程度のセキュリティが必要な状況に最適です。マイクロコントローラチップは、メモリ内の情報を追加、削除、またはその他の方法で操作できます。マイクロコントローラーは、入出力ポート、オペレーティングシステム、およびハードディスクを備えたミニチュアコンピューターのようなものです。マイクロコントローラが組み込まれたスマートカードには、大量のデータを保存し、独自のオンカード機能を実行する独自の機能があります（例：
特定のカードテクノロジーの選択は、次のようなさまざまな問題によって決まります。
アプリケーションのダイナミクス一般的な市場インフラストラクチャビジネスモデルの経済学共有アプリケーションカードの戦略
スマートカードは、次のような世界中の多くのアプリケーションで使用されています。
安全な身分証明書従業員IDバッジ、市民ID文書、電子パスポート、
運転免許証、オンライン認証装置
ヘルスケアアプリケーション市民の健康IDカード、医師IDカード、携帯型医療記録
カード
支払いアプリケーション接触型および非接触型クレジット/デビットカード、トランジット支払いカード
電気通信アプリケーション-GSM 加入者識別モジュール、電話支払いの支払い
カード
次の答えは正しくありません。
スマートカードに連絡する
連絡先のスマートカードは、スマートカードリーダーに直接接続して挿入する必要があります。
カードの表面にある導電性コンタクトプレート（通常は金メッキ）。の送信
コマンド、データ、およびカードのステータスは、これらの物理的な連絡先で行われます。
非接触型スマートカード

非接触型カードは、リーダーに近接している必要があります。リーダーとカードの両方が持っています
アンテナ、および2つは、この非接触リンクを介して無線周波数（RF）を使用して通信します。多くの
非接触型カードも、この電磁信号から内部チップの電力を引き出します。The
範囲は通常、バッテリー駆動でないカードの場合は0.5〜3インチであり、アプリケーションに最適です。
非常に高速なカードインターフェースを必要とする建物の入場や支払いなど。
コンビカード
ハイブリッドカードに似ていますが、2つではなく1セットの回路しか含まれていません。
この質問を作成するために、次の参照が使用されました。
スマートカード入門書：http ://www.smartcardalliance.org/pages/smart-cards-intro-primer

最新問題: **143**
IANAによって割り当てられたよく知られたポートは次のうちどれですか？
A. ポート0〜255
B. ポート0〜1024
C. ポート0〜1023
D. ポート0〜127
Answer: C (メーッセージを残す**)**
説明/参照：
Explanation:
0〜1023の範囲のポート番号は、既知のポートまたはシステムポートです。
不正解：
A：既知のポートの範囲は、0から255ではなく、0から1023です。
B：既知のポートの範囲は、0から1024ではなく、0から1023です。
D：既知のポートの範囲は、0から127ではなく、0から1023です。
参照：
https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

最新問題: **144**
DoD参照モデルでは、どのレイヤーがOSIトランスポートレイヤーに準拠していますか？
A. プロセス/アプリケーション層
B. インターネット層
C. ホスト間レイヤー
D. ネットワークアクセス層
Answer: C (メーッセージを残す**)**
DoD参照モデルでは、ホスト間層はOSIのトランスポート層の機能と同等です。この層には、伝送制御プロトコル（TCP）とユーザーデータグラムプロトコル（UDP）が含まれています。

* DoDプロセス/アプリケーション層は、OSIの上位3層、アプリケーション、プレゼンテーション、およびセッション層に対応します。* DoDインターネット層は、OSIのネットワーク層に対応しています。
* DoDネットワークアクセス層は、OSIモデルのデータリンク層と物理層に相当します。出典：MCSE :TCP / IP Study Guide by Todd Lammle、Monica Lammle、John Chellis（Sybex、1997）およびHandbook of Information Security Management 1999 by Micki Krause andHaroldf。ティプトン（Auerbach、1999）。

最新問題: **145**
質問に答えるには、以下の情報を参照してください。
セキュリティインシデントの調査中に、無許可であると判断された
個人は、財務情報を含むデータベースをホストするシステムにアクセスしました。
許可されていない個人によって大量の情報がコピーされたことが発見された場合、データのどの属性が侵害されていますか？
A. 整合性
B. 可用性
C. 守秘義務
D. 説明責任
Answer: C (メーッセージを残す**)**

最新問題: **146**
次のクラスのうち、裁量的保護としてTCSEC（オレンジブック）で定義されているものはどれですか？
A. C
B. B
C. A
D. D
Answer: (解答を表示する**)**
出典 :KRUTZ、Ronald L. &VINES、Russel D.、CISSP準備ガイド：
コンピュータセキュリティの10のドメインをマスターする、197ページ。
また :すべてのTCSEC「レベル」質問のソース：
http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt

最新問題: **147**
プロキシファイアウォールは、オープンシステム相互接続（OSI）モデルのどの層で動作しますか？
A. ネットワーク
B. データリンク
C. 輸送
D. アプリケーション

Answer: D (メーッセージを残す)

最新問題: **148**
スマートカードへの攻撃は、一般的にどのカテゴリに分類されますか？
A. 物理的な攻撃。
B. トロイの木馬の攻撃。
C. 論理攻撃。
D. すべての選択肢に加えて、ソーシャルエンジニアリング攻撃。
Answer: D (メーッセージを残す)
スマートカードへの攻撃は、一般に、論理攻撃、物理攻撃、トロイの木馬攻撃、ソーシャルエンジニアリング攻撃の4つのカテゴリに分類されます。

最新問題: **149**
ピッキングは、次のロックメカニズム攻撃のどれに分類されますか？
A. 不正なキー
B. 回避
C. 操作
D. シミング
Answer: C (メーッセージを残す)
ピッキングはタンブラーの操作です。

最新問題: **150**
通常の電圧を下回る長時間の電源装置は次のとおりです。
A. 電圧低下
B. 停電C.サージ
C. 障害
Answer: A (メーッセージを残す)
通常の電圧を下回る長時間の電源装置は電圧低下です。
From :HARRIS、ション、オールインワンCISSP認定試験ガイド、第3回。エディションマッグロウ-Hill / Osborne、2005年、368ページ。

最新問題: **151**
次の文を完成させます。メッセージは暗号化できます。これにより、次のことが可能になります。
A. 守秘義務
B. 否認防止
C. 認証
D. 整合性
Answer: A (メーッセージを残す)
説明/参照：

機密性により、メッセージは目的の受信者だけが読むことができます。メッセージを暗号化すると、機密性が確保されます。
さまざまな手順とアルゴリズムにより、さまざまな種類のセキュリティサービスが提供されます。
メッセージは暗号化できるため、機密性が確保されます。
▪
メッセージはハッシュ化でき、整合性を提供します
▪
メッセージはデジタル署名することができ、認証、否認防止、および整合性を提供します。
▪
メッセージは暗号化してデジタル署名することができ、機密性、認証、
▪
否認防止、および誠実さ
不正解：
B :メッセージの否認防止を提供するには、デジタル署名が必要です。暗号化だけでは否認防止は提供されません。
C :メッセージの認証を提供するには、デジタル署名が必要です。暗号化だけでは認証は提供されません。
D :メッセージの整合性を提供するにはハッシュが必要です。暗号化だけでは整合性は提供されません。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、2013、pp.829-830

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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**
プログラムを介してのみオブジェクトへのアクセスを導入するセキュリティモデルはどれですか？
A. ビバモデル
B. ベルラパドゥラモデル
C. クラークウィルソンモデル
D. 情報フローモデル
Answer: C (メーッセージを残す**)**
Clark-Wilsonモデルは完全性保護モデルでもあります。Clark-WilsonモデルはBibaの後に開発され、異なる観点から完全性保護にアプローチします。格子構造を採用するのではなく、サブジェクト/プログラムの3つの部分からなる関係を使用します。/ objectはトリプルと呼ばれます。サブ

ジェクトはオブジェクトに直接アクセスできません。オブジェクトは、プログラムを介してのみアクセスできます。」Pg 347 Tittel :CISSP学習ガイド

最新問題: **153**
データベースに関して、コードと分析の再利用が容易で、メンテナンスが少ないという特徴があるのは次のうちどれですか？
A. オブジェクト指向データベース（OODB）
B. オブジェクトリレーショナルデータベース（ORDB）
C. リレーショナルデータベース
D. データベース管理システム（DBMS）
Answer: A (メーッセージを残す**)**
OODBには、コードと分析の再利用が容易で、メンテナンスが少なく、問題の分析から設計と実装への移行が容易であるという特徴があります。
出典 :KRUTZ、Ronald L.＆VINES、Russel D.、CISSP準備ガイド :マスタリング
コンピュータセキュリティの10のドメイン、2001年、John Wiley＆Sons、47ページ。

最新問題: **154**
次のうち、コモンローに基づく法律のカテゴリではないものはどれですか
システム？
A. 行政/規制法
B. 刑法
C. 大陸法
D. 派生法
Answer: (解答を表示する**)**
正解は派生法です。それは気を散らすものであり、他のすべての答えはコモンローの下のカテゴリーです。

最新問題: **155**
以下のどのタイプのルーティングが、そのルーティングテーブルを一般的にブロードキャストしますか
毎分他のすべてのルーターへの情報？
A. 動的制御プロトコルルーティング
B. 静的ルーティング
C. 距離ベクトルルーティング
D. リンクステートルーティング
Answer: (解答を表示する**)**
距離ベクトルルーティングは、ルーティング情報プロトコルを使用します
（RIP）ルーティング情報の動的テーブルを維持する
定期的に更新されます。それは最も古く、最も一般的なタイプです
動的ルーティング。

*静的ルーティング。ルーターの構成ファイルで特定のルートを定義し、ルーターがルート情報を動的に交換する必要はありません。
*リンクステートルーター、距離ベクトルルーターのように機能しますが、他のすべてのルーターのリンクのコピーを維持することにより、ルーティングテーブルを構築するときにのみ直接情報を使用します
状態プロトコル（SP）フレーム。これにより、ルーティングエラーが排除され、収束時間が大幅に短縮されます。
* Answer Dynamic ControlProtocolRoutingは気を散らすものです。
出典：ChrisBrentonによるMasteringNetwork Security（Sybex、1999）。

最新問題: **156**
次の質問のうち、監査証跡をカバーする統制の評価に最も役立つ可能性が低いのはどれですか？
A. 監査証跡はユーザーアクションのトレースを提供しますか？
B. インシデントは解決されるまで監視および追跡されますか？
C. オンラインログへのアクセスは厳密に管理されていますか？
D. アクセス制御機能を管理するセキュリティ担当者と監査証跡を管理するセキュリティ担当者の間に職務の分離はありますか？
Answer: B (メーッセージを残す**)**
説明/参照：
Explanation:
監査証跡は、システムまたはアプリケーションプロセスごと、およびユーザーアクティビティごとのシステムアクティビティの記録を維持します。適切なツールと手順を組み合わせることで、監査証跡は、個人の説明責任、イベントの再構築、侵入の検出、および問題の特定の手段を提供できます。監査証跡管理は技術管理と見なされます。
インシデントの監視と追跡は、インシデント対応機能に関連する運用管理です。
したがって、インシデントが解決されるまで監視および追跡されているかどうかを尋ねても、監査証跡をカバーする統制を評価するのに役立ちません。
不正解：
A：監査証跡は、ユーザーアクションのトレースを提供する必要があります。これについて質問することは、監査証跡をカバーする統制を評価するのに役立ちます。
C：オンラインログへのアクセスは厳密に管理する必要があります。これについて質問することは、監査証跡をカバーする統制を評価するのに役立ちます。
D：アクセス制御機能を管理するセキュリティ担当者と監査証跡を管理するセキュリティ担当者の間で職務を分離する必要があります。これについて質問することは、監査証跡をカバーする統制を評価するのに役立ちます。

最新問題: **157**
次のうち、独自の暗号化アルゴリズムとして設計されていないものはどれですか？
A. RC2
B. RC4

C. フグ
D. スキップジャック
Answer: C (メーッセージを残す**)**
Blowfishは、DESまたはIDEAの特許を取得していない、ライセンスやロイヤリティフリーの代替品として1993年にBruce Schneierによって設計された可変長キー（32～448ビット）を備えた対称ブロック暗号です。以下の属性を参照してください。
ブロック暗号：64ビットブロック
可変キー長：32ビットから448ビット
ブルースシュナイアーによるデザイン
DESやIDEAよりもはるかに高速
特許を取得しておらず、ロイヤリティフリー
ライセンスは必要ありません
利用可能な無料のソースコード
Rivest Cipher#2（RC2）は、Ronによって発明された独自の可変キー長ブロック暗号です。
RSA Data Security、Inc.のRivest
Rivest Cipher#4（RC4）は、Ronによって発明された独自の可変キー長ストリーム暗号です。
RSA Data Security、Inc.のRivest
スキップジャックアルゴリズムは、ブロックサイズが64ビットでキーサイズが80ビットのタイプIIブロック暗号[NIST]であり、NSAによって開発され、以前は米国で分類されていました。
国防総省の「秘密」レベル。NSAは1998年6月23日に、次のように発表しました。
スキップジャックは機密解除されていました。
参照：
RSAラボラトリーズ
http://www.rsa.com/rsalabs/node.asp?id=2250
RFC2828-インターネットセキュリティ用語集
http://www.faqs.org/rfcs/rfc2828.html

最新問題**: 158**
セキュアアクセスモデルに関して正しいのは次のうちどれですか？
A. 安全な情報をより安全なユーザーに流すことはできません。
B. 安全性の低いユーザーに安全な情報を流すことはできません。
C. 安全性の低いユーザーに安全な情報が流れる可能性があります。
D. 選択肢はありません。
Answer: (解答を表示する**)**
アクセス制御リストや機能などのアクセス制限では不十分な場合があります。場合によっては、情報の所有者よりも高い権限によって、情報をさらに厳しくする必要があります。たとえば、官公庁の極秘文書の所有者は、多くのユーザーが利用できる情報を利用できると見なすかもしれませんが、彼のマネージャーは、情報をそれ以上に制限する必要があることを知っているかもしれません。この場合、情報の流れを制御する必要があります。安全性の低いユーザーに安全な情報を流すことはできません。

最新問題: **159**
質問に答えるには、以下の情報を参照してください。
セキュリティインシデントの調査中に、許可されていない個人が財務情報を含むデータベースをホストするシステムにアクセスしたと判断されました。
許可されていない個人によって大量の情報がコピーされたことが発見された場合、データのどの属性が侵害されていますか？
A. 説明責任
B. 可用性
C. 守秘義務
D. 整合性
Answer: C (メーッセージを残す**)**

最新問題: **160**
アクセス制御トリプルを使用し、職務の分離も必要なセキュリティモデルはどれですか？
A. DAC
B. ラティス
C. クラークウィルソン
D. ベルラパドゥラ
Answer: C (メーッセージを残す**)**
次の答えは正しくありません。
DAC
ベルラパドゥラ
格子
この質問を作成するために、次の参照が使用されました。
義務の分離は、必然的にコンピュータシステムの外部の条件によって決定されます。
Clark-Wilsonスキームには、アクセス制御トリプルで表現されているように、要件として職務分離の維持が含まれています。
強制は、アクセス制御トリプルからのユーザーIDを使用して、ユーザーごとに行われます。

最新問題: **161**
RSAと比較して、楕円曲線暗号（ECC）について正しいのは次のうちどれですか？
A. 数学的に安全であることが証明されています。
B. 数学的に安全性が低いことが証明されています。
C. 同等のセキュリティを実現するには、より長いキーが必要になると考えられています。
D. 同等のセキュリティを実現するには、より短いキーが必要になると考えられています。
Answer: D (メーッセージを残す**)**
The_answer：同等のセキュリティを実現するには、より短いキーが必要になると考えられています。

一部の専門家は、キー長160ビットのECCは、キー長1024ビットのRSAと同等であると考えています。
次の答えは正しくありません。数学的に安全性が低いことが証明されています。
ECCはRSAよりも多かれ少なかれ安全であることが証明されていません。ECCはより新しいのでRSA、一部の人はリスクが高いと考えていますが、これは単なる一般的な評価であり、数学的な議論に基づくものではありません。
より安全であることが数学的に証明されています。ECCはRSAよりも多かれ少なかれ安全であることが証明されていません。ECCはRSAよりも新しいため、一部の人はリスクが高いと考えていますが、これは単なる一般的な評価であり、数学的な議論に基づくものではありません。
同等のセキュリティを実現するには、より長いキーが必要になると考えられています。それどころか、RSAの同等のセキュリティには、より短いキーが必要であると考えられています。
ション・ハリス、AIOv5pg719は次のように述べています。
「ほとんどの場合、キーが長いほど、より多くの保護が提供されますが、ECCは、RSAが必要とするものよりも短いキーサイズで同じレベルの保護を提供できます。」
この質問を作成するために、次の参照が使用されました。
ISC2 OIG、2007年p。258
ション・ハリス、AIO v5 pg719

最新問題: **162**
調査で押収された各アイテムを特定する文書は、次のうちどれですか。これには、押収された日時、アイテムを押収した人の氏名と署名またはイニシャル、およびアイテムの詳細な説明が含まれます。
A. プロパティブック
B. CoC形式
C. 検索令状の返却
D. 証拠タグ
Answer: (解答を表示する**)**
セクション :ソフトウェア開発のセキュリティ

最新問題: **163**
次のファイルのうち、セキュリティ管理者を読み取り専用アクセスに制限する必要があるのはどれですか？
A. システムログ
B. セキュリティパラメータ
C. ユーザープロファイル
D. ユーザーパスワード
Answer: A (メーッセージを残す**)**

最新問題: **164**

転送されるデータの整合性を確保しながら、特定の転送を開始したソースを認証することにしました。これは次の方法で実行できます。
A. 送信者に秘密鍵を使用してメッセージを暗号化させる。
B. 送信者に自分の秘密鍵でハッシュを暗号化させる。
C. 送信者に対称鍵を使用してメッセージを暗号化させる。
D. 送信者に公開鍵を使用してハッシュを暗号化させる。
Answer: B (メーッセージを残す**)**
共有キーを使用して特定のメッセージのハッシュを暗号化する代わりに、送信者の秘密キーを使用してメッセージのハッシュ値を暗号化します。これは、メッセージにデジタル署名する行為です。
デジタル署名は、送信者の認証と送信者のメッセージの整合性を提供します。
メッセージがハッシュ関数に入力されます。次に、送信者の秘密鍵を使用してハッシュ値が暗号化されます。これらの2つのステップの結果、デジタル署名が生成されます。受信者は、署名者の公開鍵を使用してハッシュ値を復号化することでデジタル署名を検証し、メッセージに対して同じハッシュ計算を実行して、完全に一致するハッシュ値を比較できます。ハッシュ値が同じである場合、署名は有効です。
次の答えは正しくありません。
送信者に公開鍵を使用してハッシュを暗号化させる。送信者だけが自分の秘密鍵を使用してコールド復号化し、他の誰も使用しないため、これは何のメリットもありません。
publickキーを使用した暗号化は、機密性のみを提供し、他のサービスは提供しません。
送信者に自分の秘密鍵を使用してメッセージを暗号化させる。これは近いですが、十分ではありません。ソースの信頼性のみを提供します。
送信者に対称鍵を使用してメッセージを暗号化させる。これは提供するだけです
守秘義務。
この質問を作成するために、次の参照が使用されました。
Hernandez CISSP、Steven（2012-12-21）。CISSP CBKの公式（ISC）2ガイド、サードEdition（ISC）2 Press）Kindle Locations 14885-14889）。AuerbachPublications。Kindle版。

最新問題: **165**
公開鍵暗号は、公開鍵署名と？を使用して整合性検証を提供します。
A. 安全なハッシュ
B. 秘密鍵の署名
C. セッションキー
D. ゼロ知識
Answer: A (メーッセージを残す**)**

最新問題: **166**

企業は、米国国立標準技術研究所（NIST）の次の機能で上位にランク付けされました：保護 検出、応答、および回復。ただし、成熟度が低いのは、識別機能が原因でした。プロセスを個別に分析する場合、この会社が改善する必要がある管理カテゴリは次のうちどれですか？
A. 資産管理、ビジネス環境、ガバナンス、およびリスク評価
B. 異常とイベント、セキュリティの継続的な監視と検出のプロセス
C. アクセス制御、認識とトレーニング、データのセキュリティとメンテナンス
D. 復旧計画、改善、コミュニケーション
Answer: A (メーッセージを残す)

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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**
ハードウェアRAIDの実装は通常次のとおりです。
A. プラットフォームに依存しません。
B. プラットフォームに依存します。
C. オペレーティングシステムに依存します。
D. ソフトウェアに依存します。
Answer: A (メーッセージを残す)
説明/参照：
Explanation:
RAIDは、ハードウェアまたはソフトウェアのいずれかで実装できます。それぞれのタイプには、独自の問題と利点があります。ハードウェアRAIDの実装は通常、プラットフォームに依存しません。サーバーのオペレーティングシステム（OS）の下で実行され、通常、OSがNovell、NT、またはUnixのいずれであるかは関係ありません。ハードウェア実装は、インテリジェントコントローラカードでの計算に独自の中央処理装置（CPU）を使用します。サーバーにハードウェアの冗長性を提供するために、これらのカードを複数インストールすることができます。RAIDレベル3および5は、ハードウェア上でより高速に実行されます。RAIDのソフトウェア実装は、ファイルサーバー上のオペレーティングシステムの一部として実行されることを意味します。
不正解：
B：ハードウェアRAIDの実装はプラットフォームに依存しません。
C：ハードウェアRAIDの実装は、オペレーティングシステムに依存しません。
D：ハードウェアRAIDの実装はソフトウェアに依存しません。
参照：

Krutz、Ronald L. and Russell Dean Vines、CISSP Prep Guide :Mastering the CISSP and ISSEP Exams、2nd Edition、Wiley Publishing、Indianapolis、2004、p。145

最新問題**: 168**
目立たないマークまたはラベルをデジタルデータのビットとして不可分に埋め込み、後でマークを検出または抽出するためのコンピューティング技術として最もよく定義できるのは、次のうちどれですか？
A. ステガノグラフィ
B. 電子透かし
C. デジタルエンベロープ
D. デジタル署名
Answer: B (メーッセージを残す**)**
説明/参照：
Explanation:
電子透かしは、「目立たないマークまたはラベルをデジタルデータ（テキスト、グラフィックス、画像、ビデオ、またはオーディオ）にビットとして不可分に埋め込み、後でマークを検出または抽出するためのコンピューティング技術」と定義されています。
「電子透かし」、つまり埋め込まれたビットのセットは、隠されている場合があり、通常は認識できず、常に目立たないように意図されています。使用する特定の技術に応じて、電子透かしは、所有権の証明、複製の制御、配布のトレース、データの整合性の確保、および知的財産権を保護するための他の機能の実行に役立ちます。
不正解：
A :ステガノグラフィは、別のメディアタイプのデータを隠す方法であるため、データの存在そのものが隠されます。電子透かしは、ステガノグラフィの一種と見なされています。ただし、ステガノグラフィは質問で説明されているものではありません。
C :デジタルエンベロープは、メッセージが対称鍵で暗号化され、対称鍵が非対称鍵で暗号化されるハイブリッド暗号化を説明するために使用される別の用語です。これは質問で説明されていることではありません。
D :デジタル署名は、メッセージ、ソフトウェア、またはデジタルドキュメントの信頼性と整合性を検証するために使用される数学的な手法です。これは質問で説明されていることではありません。
参照：
http://tools.ietf.org/html/rfc4949

最新問題**: 169**
重要なWebベースのシステムで、入力の検証と例外処理の脆弱性が発見されました。コントロールをすばやく実装するのに最も適しているのは次のうちどれですか？
A. アプリケーションのソースコードにパッチを適用する
B. 侵入検知システム（IDS）をインストールする
C. アプリケーション層ファイアウォールに新しいルールを追加します

D. サービスへのアクセスをブロックする
Answer: C (メーッセージを残す**)**

最新問題**: 170**
以下の選択は、監査メカニズムのセキュリティ目標ではありませんか？
A. 従業員の生産出力レコードを確認します
B. 加害者がシステム保護メカニズムを回避しようとするのを阻止する
C. 個々のオブジェクトへのアクセスパターンを確認する
D. ユーザーが自分よりも高い特権を持つ機能を引き受ける時期を発見する
Answer: (解答を表示する**)**
コンピュータシステムの監査メカニズムには、5つの重要なセキュリティ目標があります。
1.監査メカニズムでは、個々のオブジェクトへのアクセスパターン、特定のプロセスと個人のアクセス履歴、およびシステムとその有効性によってサポートされるさまざまな保護メカニズムの使用を確認できる必要があります。2
2.ユーザーと部外者の両方の発見を許可し、保護メカニズムをバイパスする試みを繰り返します。
3.ユーザーが自分よりも高い特権を持つ機能を引き受けたときに発生する可能性のある特権の使用の検出を許可する
または彼女自身、つまりプログラマーから管理者へ。この場合、セキュリティ制御のバイパスはないかもしれませんが、それでも違反は可能になります。
4.システム保護メカニズムを迂回しようとする実行者の習慣的な試みに対する抑止力として機能します。ただし、抑止力として機能するには、加害者は、監査メカニズムの存在と、システム保護メカニズムをバイパスする試みを検出するための監査メカニズムの積極的な使用を認識している必要があります。
5.記録および検出された保護メカニズムをバイパスしようとする追加の形式のユーザー保証を提供します。3保護メカニズムをバイパスする試みが成功した場合でも、監査証跡は、評価を支援する能力によって保証を提供します。違反によって行われた損傷。これにより、損傷を制御するシステムの能力が向上します。
出典 :NCSC-TG-001信頼できるシステムの監査を理解するためのガイド[Tan Book]、およびGligor、Virgil D.、信頼できる施設の管理と監査のガイドライン、メリーランド大学、1985年。

最新問題**: 171**
SSLはどのような暗号化技術を利用していますか？
A. 秘密鍵または対称鍵
B. ハイブリッド（対称と非対称の両方）
C. 公開鍵
D. 秘密鍵
Answer: B (メーッセージを残す**)**
SSLは公開鍵暗号を使用してセッション鍵を保護し、セッション鍵（秘密鍵）は相互に通信する両当事者間で行われるセッション全体を保護するために使用されます。

SSLプロトコルは、もともとNetscapeによって開発されました。バージョン1.0が公開されることはありませんでした。バージョン2.0は1995年2月にリリースされましたが、SSLバージョン3.0の設計につながる多くのセキュリティ上の欠陥が含まれていました」。SSLバージョン3.0、でリリース
1996年は、PaulKocherが共同で作成したプロトコルを完全に再設計したものです。
NetscapeのエンジニアであるPhilKarltonとAlanFreier。
他のすべての答えは正しくありません

最新問題: **172**
OSIモデルのレイヤー2には、2つのサブレイヤーがあります。それらのサブレイヤーとは何ですか？また、そのレイヤーのテクノロジーを説明する2つのIEEE標準は何ですか？
A. LCLおよびMAC; IEEE8022および8023
B. LCLおよびMAC; IEEE8021および8023
C. ネットワークとMAC; IEEE8021および8023
Answer: A (メーッセージを残す**)**
OSIモデルのデータリンク層または層2は、ヘッダーの追加を担当します
ローカルエリアネットワークまたはワイドエリアネットワーク用のパケットを準備するためのパケットへのトレーラー
適切な回線伝送のためのテクノロジーバイナリフォーマット。
レイヤー2は、2つの機能サブレイヤーに分割されています。
上位サブレイヤーは論理リンク制御（LLC）であり、IEEE8022仕様で定義されています。
データリンク層のすぐ上にあるネットワーク層と通信します。
LLCの下には、メディアアクセス制御（MAC）サブレイヤーがあります。これは、
物理層のプロトコル要件。
したがって、この層の仕様は、物理層のテクノロジーによって異なります。
イーサネットのIEEEMAC仕様は8023、トークンリングは8025、無線LANは80211、および
すぐ。80211や80216などのIEEE標準への参照が表示されている場合は、
プロトコルスタックのデータリンク層のMACサブレイヤーで動作するプロトコル。
次の答えは正しくありません：LCLとMAC。LCLは注意をそらすものであるため、IEEE8022および8023は正しくありません。データリンク層の上位サブレイヤーの正しい頭字語はLLCです。これは、論理リンク制御の略です。LLCは、多重化およびフロー制御メカニズムを提供することにより、マルチポイントネットワーク内でのネットワークプロトコルの共存と、同じネットワークメディア上でのそれらの転送を可能にします。LCLおよびMAC; LCLは注意をそらすものであるため、IEEE8021および8023は正しくありません。データリンク層のサブレイヤーは、論理リンク制御（LLC）とメディアアクセス制御（MAC）です。さらに、LLCは8021ではなくIEEE 8022仕様で定義されています。IEEE8021仕様は、MACおよびLLC層の上のプロトコル層に関係しています。LAN / MANアーキテクチャ、ネットワーク管理、LANとWAN間のインターネットワーキング、およびリンクセキュリティなど。ネットワークおよびMAC。ネットワークはデータリンク層のサブレイヤーではないため、IEEE8021および8023は正しくありません。データリンク層のサブレイヤー

は、論理リンク制御（LLC）とメディアアクセス制御（MAC）です。LLCは、ネットワーク層（データリンク層のすぐ上の層）とMACサブ層の間に位置します。また、LLCはIEEE8021ではなくIEEE8022仕様で定義されています。今説明したように、8021規格は、LAN / MANアーキテクチャ、ネットワーク管理、LANとWAN間のインターネットワーキング、およびリンクセキュリティの領域に対応しています。IEEE8021グループの4つのアクティブなタスクグループインターネットワーキング、セキュリティ、オーディオ/ビデオブリッジング、およびデータセンターブリッジングです。データリンク層のサブレイヤーは、論理リンク制御（LLC）とメディアアクセス制御（MAC）です。LLCは、ネットワーク層（データリンク層のすぐ上の層）とMACサブ層の間に位置します。また、LLCはIEEE8021ではなくIEEE8022仕様で定義されています。今説明したように、8021規格は、LAN / MANアーキテクチャ、ネットワーク管理、LANとWAN間のインターネットワーキング、およびリンクセキュリティの領域に対応しています。IEEE8021グループの4つのアクティブなタスクグループインターネットワーキング、セキュリティ、オーディオ/ビデオブリッジング、およびデータセンターブリッジングです。データリンク層のサブレイヤーは、論理リンク制御（LLC）とメディアアクセス制御（MAC）です。LLCは、ネットワーク層（データリンク層のすぐ上の層）とMACサブ層の間に位置します。また、LLCはIEEE8021ではなくIEEE8022仕様で定義されています。今説明したように、8021規格は、LAN / MANアーキテクチャ、ネットワーク管理、LANとWAN間のインターネットワーキング、およびリンクセキュリティの領域に対応しています。IEEE8021グループの4つのアクティブなタスクグループインターネットワーキング、セキュリティ、オーディオ/ビデオブリッジング、およびデータセンターブリッジングです。
この質問を作成するために、次の参照が使用されました：http://en.wikipedia.org/wiki/OSI_model

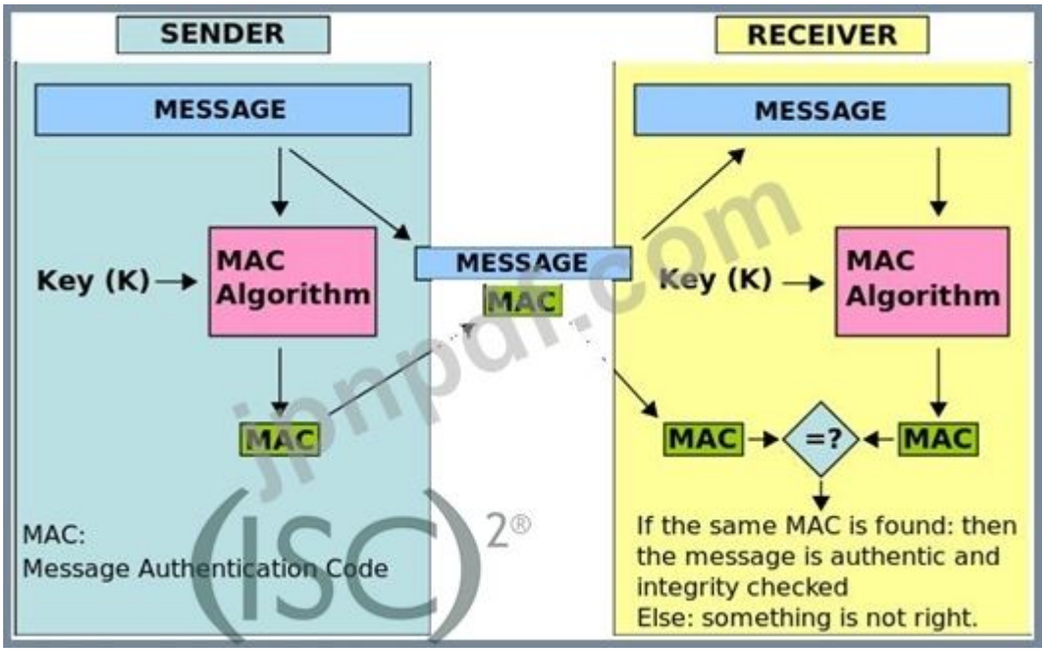
最新問題: **173**
次のテスト方法のうち、アプリケーションの内部構造または動作を調べるものはどれですか？
A. ホワイトボックステスト
B. 並列テスト
C. 回帰テスト
D. パイロットテスト
Answer: A (メーッセージを残す**)**
ホワイトボックステスト（クリアボックステスト、ガラスボックステスト、透明ボックステスト、構造テストとも呼ばれます）は、アプリケーションの機能（つまり、ブラックボックス）ではなく、アプリケーションの内部構造または動作をテストするソフトウェアをテストする方法です。テスト）。ホワイトボックステストでは、システムの内部的な視点とプログラミングスキルを使用して、テストケースを設計します。テスターは、入力を選択してコード内のパスを実行し、適切な出力を決定します。これは、回路内のノードのテスト、たとえばインサーキットテスト（ICT）に似ています。ホワイトボックステストは、ソフトウェアテストプロセスのユニット、統合、およびシステムレベルで適用できます。従来のテスターは、ホワイトボックステストをユニットレベルで実行されると考える傾向がありましたが、今日では、統合およびシステムテストでより頻繁に使用されています。ユニット内のパス、統合中のユニット間のパス、およびシステムレベルのテスト中

のサブシステム間のパスをテストできます。このテスト設計の方法では、多くのエラーや問題を発見できますが、仕様の実装されていない部分や不足している要件を見逃す可能性があります。
試験については、以下の情報を知っておく必要があります。アルファおよびベータテスト-アルファバージョンは初期バージョンであり、テストのために内部ユーザーに送信されるアプリケーションシステムの初期バージョンです。アルファ版には、最終版で計画されているすべての機能が含まれていない場合があります。通常、ソフトウェアは、終了したと見なされる前に2段階のテストに進みます。最初の段階はアルファテストと呼ばれ、多くの場合、ソフトウェアを開発している組織内のユーザーによってのみ実行されます。第2段階はベータテストと呼ばれ、ユーザー受け入れテストの一種であり、通常、限られた数の外部ユーザーが関与します。ベータテストはテストの最終段階であり、通常は実際の露出を伴い、製品のベータバージョンを独立したベータテストサイトに送信するか、関心のあるユーザーに無料で提供します。
パイロットテスト-システムの特定の事前定義された側面に焦点を当てた予備テスト。です
他のテスト方法を置き換えることを意図したものではなく、
システム。概念実証は初期のパイロットテストです-通常は暫定プラットフォーム上で、基本的なものだけを使用します
機能。
ホワイトボックステスト-ソフトウェアプログラムロジックの有効性を評価します。具体的には、テストデータは
プログラムの特定の論理パスの手順の精度または条件を決定する際に使用されます。でも
大規模な情報システムで考えられるすべての論理パスをテストすることは実行不可能であり、コストがかかります
禁止的であるため、選択的にのみ使用されます。
ブラックボックステスト-のコンポーネントのテストに関連する整合性ベースのテスト形式
特定の内部に関係なく、情報システムの「機能的な」運用効率
プログラム構造。統合およびユーザー受け入れテストに適用できます。
機能/検証テスト-システムテストに似ていますが、多くの場合、
詳細な要件に対するシステムの機能。
構築されたものは、顧客の要件にトレーサブルです。
回帰テスト-テストシナリオまたはテスト計画の一部を再実行して、
その変更または修正によって新しいエラーが発生することはありません。回帰テストで使用されるデータ
元のデータと同じである必要があります。
並列テスト-これは、テストデータを2つのシステムにフィードするプロセスです変更されたシステム
代替システムと結果の比較。
社会性テスト-これらのテストの目的は、新しいシステムまたは変更されたシステムが次のことができることを確認することです。
既存のシステムに悪影響を与えることなく、ターゲット環境で動作します。これはカバーする必要があります

一次アプリケーション処理を実行し、他のシステムとのインターフェースをとるプラットフォームだけではありません
ただし、クライアントサーバーおよびWeb開発では、デスクトップ環境が変更されます。多数アプリケーションはユーザーのデスクトップで、場合によっては同時に実行される可能性があるため、テストすることが重要です。
新しいダイナミックリンクライブラリ（DLL）のインストール、オペレーティングシステムレジストリの作成、または
構成ファイルの変更、および場合によっては余分なメモリ使用率。
次の答えは正しくありません。
並列テスト-これは、テストデータを2つのシステムにフィードするプロセスです変更されたシステム
代替システムと結果の比較。
回帰テスト-テストシナリオまたはテスト計画の一部を再実行して、
その変更または修正によって新しいエラーが発生することはありません。回帰テストで使用されるデータ
元のデータと同じである必要があります。
パイロットテスト-システムの特定の事前定義された側面に焦点を当てた予備テスト。これは、他のテスト方法を置き換えることを意図したものではなく、システムの限定的な評価を提供することを目的としています。概念実証は初期のパイロットテストです通常は暫定プラットフォーム上で、基本的な機能のみを使用します
この質問を作成するために、次の参照が使用されました。CISAレビューマニュアル2014ページ番号167CISSPCBK第3版の公式ISC2ガイドページ番号176
トピック2、通信およびネットワークセキュリティ

最新問題: **174**
次のうち、既知のタイプのメッセージ認証コード（MAC）ではないものはどれですか？
A. キー付きハッシュメッセージ認証コード（HMAC）
B. DES-CBC
C. 署名ベースのMAC（SMAC）
D. ユニバーサルハッシュベースのMAC（UMAC）
Answer: C (メーッセージを残す**)**
シグニチャベースのMACのようなものはありません。リストの中で間違った選択であるため、この質問に対する最良の答えです。
メッセージ認証コード（MAC）とは何ですか？
暗号化では、暗号化チェックサムとも呼ばれるMAC（メッセージ認証コード）は、秘密鍵を使用して生成され、メッセージに追加されるデータの小さなブロックです。メッセージを受信すると、受信者は秘密鍵を使用して独自のMACを生成できるため、メッセージが誤ってまたは意図的に送信中に変更されていないことがわかります。もちろん、この保証は、他の誰も秘密鍵にアクセスできないという2つの当事者の信頼と同じくらい強力です。
MACはメッセージの小さな表現であり、次の特徴があります。

MACは、それを生成するメッセージよりもはるかに小さいです。
MACが与えられた場合、それを生成したメッセージを計算することは実用的ではありません。
MACとそれを生成したメッセージを考えると、同じMACを生成する別のメッセージを見つけることは実用的ではありません。
MAC値の作成を示すウィキペディアの以下の図を参照してください。



メッセージ認証コードMACHMAC
上記の例では、メッセージの送信者がMACアルゴリズムを実行して、MACデータタグを生成します。次に、メッセージとMACタグが受信者に送信されます。次に、受信者は、同じキーを使用して同じMACアルゴリズムを介して送信のメッセージ部分を実行し、2番目のMACデータタグを生成します。次に、受信者は、送信で受信した最初のMACタグを2番目に生成されたMACタグと比較します。
それらが同一である場合、受信者は、メッセージの整合性が損なわれておらず、送信中にメッセージが変更または改ざんされていないことを安全に想定できます。
ただし、受信者がリプレイ攻撃を検出できるようにするには、メッセージ自体に、この同じメッセージを1回だけ送信できることを保証するデータが含まれている必要があります タイムスタンプ、シーケンス番号、ワンタイムMACの使用など)。そうしないと、攻撃者は、その内容を理解していなくても、このメッセージを記録して後で再生し、元の送信者と同じ結果を生成する可能性があります。
注 :MAC値を生成する方法はたくさんあります。以下に、いくつかの実装の短いリストを示します。
この質問に対する間違った答えは次のとおりです。
それらはすべて実際のタイプのMAC実装であるため、すべて間違った答えでした。
DES-CBCの場合、MACはCBCモードのDESアルゴリズムを使用して生成され、秘密のDESキーは送信者と受信者によって共有されます。MACは、実際には、アルゴリズムによって生成された暗号文の最後のブロックにすぎません。このデータブロック 64ビット)は、暗号化されていないメッセージに添付され、遠端に送信されます。MAC自体への攻撃を防ぐために、暗号化されたデータの

以前のブロックはすべて破棄されます。受信者は、共有する秘密のDESキーを使用して、自分のMACを生成するだけで、メッセージの整合性と認証を確保できます。彼は、メッセージのどこかでビットが変更された場合、CBCのチェーン機能がデータの最後のブロックを大幅に変更するため、メッセージが変更されていないことを知っています。秘密鍵を持っているのは他の1人だけなので、彼はメッセージの送信元（認証）を知っています。

キー付きハッシュメッセージ認証コード（HMAC）は、暗号化ハッシュ関数と秘密の暗号化キーを組み合わせたメッセージ認証コード（MAC）を計算するための特定の構造です。他のMACと同様に、データの整合性とメッセージの認証の両方を同時に検証するために使用できます。MD5、SHA-1などの任意の暗号化ハッシュ関数を、HMAC; 結果として得られるMACアルゴリズムは、それに応じてHMAC-MD5またはHMAC-SHA1と呼ばれます。

HMACの暗号化強度は、基になるハッシュ関数の暗号化強度、そのハッシュ出力のサイズ、およびキーのサイズと品質に依存します。

ユニバーサルハッシュ（UMAC）に基づくメッセージ認証コードは、ある秘密の（ランダムな）プロセスに従ってハッシュ関数のクラスからハッシュ関数を選択し、それをメッセージに適用することで計算されるメッセージ認証コード（MAC）の一種です。

結果のダイジェストまたはフィンガープリントは、使用されるハッシュ関数のIDを隠すために暗号化されます。他のMACと同様に、データの整合性とメッセージの信頼性の両方を同時に検証するために使用できます。UMACはRFC4418で指定されており、証明可能な暗号強度を備えており、通常、他のMACよりもはるかに計算量が少なくなります。

MicMac（混同）とMICおよびMACとは何ですか？

メッセージ整合性コード（MIC）という用語は、特に通信において、MACという用語の代わりに使用されることがよくあります。MACの頭字語は伝統的にメディアを表します。

ネットワークに言及するときのアクセス制御。ただし、一部の作成者は、MICをMACとは明らかに異なる用語として使用しています。この用語の使用法では、MIC操作は秘密鍵を使用しません。このセキュリティの欠如は、メッセージの整合性を測定するために使用することを目的としたMICは、暗号化するか、改ざんから保護する必要があることを意味します。MICアルゴリズムは、同じアルゴリズムを使用して両方を生成すると仮定すると、特定のメッセージが常に同じMICを生成するように作成されます。逆に、MACアルゴリズムは、同じメッセージ、秘密鍵、および初期化ベクトルが同じアルゴリズムに入力された場合にのみ、一致するMACを生成するように設計されています。MICは秘密鍵を使用しないため、MICを単独で使用した場合、メッセージの整合性のゲージの信頼性ははるかに低くなります。

MAC。MACは秘密鍵を使用するため、同じレベルの保証を提供するために必ずしも暗号化する必要はありません。

この質問に使用される参照：

Hernandez CISSP、Steven（2012-12-21）。CISSP CBKの公式（ISC）2ガイド、サードEdition（ISC）2 Press）Kindle Locations 15799-15815）。AuerbachPublications。Kindle版。

と

http://en.wikipedia.org/wiki/Message_authentication_code
と
http://tools.ietf.org/html/rfc4418

最新問題: **175**
磁気媒体に損傷が発生し始めるのはどの温度ですか？
A. 華氏100度または摂氏37'7度
B. 華氏125度または摂氏51.66度
C. 華氏150度または摂氏65,5度
D. 華氏175度または摂氏79,4度
Answer: A (メーッセージを残す**)**
磁気媒体は華氏100度または摂氏37度7度の影響を受けます。
ディスクは華氏150度または摂氏65,5度で損傷しています
華氏175度または摂氏79,4度のコンピューター機器、および
華氏350度または摂氏176.66度の紙製品。
出典 :ROTHKE、Ben、CISSPCBKドメイン10のレビュープレゼンテーション。

最新問題: **176**
次の言語のうち、オブジェクト指向言語ではないものはどれですか？
A. Lisp
B. C ++
C. Simula 67
D. Smalltalk
Answer: A (メーッセージを残す**)**
リスト処理用のLispは、処理する関数型言語です
数字ではなく記号式。人工的に使用されます
インテリジェンスフィールド。他の回答で引用されている言語は
オブジェクト指向言語。

最新問題: **177**
次の質問のうち、物理的および環境的保護の評価に役立つ可能性が低いのはどれですか？
A. エントリーコードは定期的に変更されますか？
B. 適切な消火および防止装置が設置され、機能していますか？
C. 許可されていない個人が印刷物や電子情報を読み取ったり、コピーしたり、変更したり、盗んだりできないようにするプロセスはありますか？
D. データ伝送ラインへの物理的アクセスは制御されていますか？
Answer: (解答を表示する**)**
物理的セキュリティと環境セキュリティは運用管理の一部であり、システム、建物、および関連するサポートインフラストラクチャを物理的環境に関連する脅威から保護するために講じられる対

策です。上記のすべての質問は、許可されていない個人が情報にアクセスできないようにするプロセスに関する質問を除いて、物理的および環境的保護を評価するのに役立ちます。
出典 :SWANSON、Marianne、NIST Special Publication 800-26、Security Self-
情報技術システムの評価ガイド、2001年11月 (ページA-21から
A-24)。

最新問題: **178**
予防技術管理は、システムの整合性と可用性をどのように保護しますか？
A. スレッド数のみを制限します。
B. システム変数の数を制限する。
C. 関数呼び出しの数のみを制限する。
D. ユーザーやプロセスの数を制限する。
Answer: D (メーッセージを残す**)**
予防的技術管理は、システムリソースにアクセスできるユーザーまたは対象、および許可されるアクセスの種類を制限する技術的な方法です。その目的は、OSおよびその他のシステムを不正な変更または操作から保護することです。通常、オペレーティングシステムに組み込まれている場合もあれば、アプリケーションやプログラムの一部、アドオンのセキュリティパッケージ、またはコンピュータ間の通信を規制するための特別なコンポーネントの場合もあります。また、ユーザーやプロセスの数を制限することにより、整合性と可用性を保護します。これらの管理はまた、機密情報が許可されていない人に開示されるのを防ぎます。

最新問題: **179**
テクノロジ環境のリカバリサイト戦略は、リカバリを完了する必要がある前に組織が許容できるダウンタイムの量によって異なります。代替サイトが内部でスタンバイ対応であり、アプリケーションの実行に必要なすべてのテクノロジーと機器を備えている戦略を何と呼びますか？
A. 外部ホットサイト
B. ウォームサイト
C. 内部ホットサイト
D. デュアルデータセンター
Answer: C (メーッセージを残す**)**
内部ホットサイトこのサイトは、そこに配置されたアプリケーションを実行するために必要なすべてのテクノロジーと機器を備えたスタンバイ対応です。プランナーは、サーバーのベアメタル回復を実行しなくても、ホットサイト回復でアプリケーションを効果的に再起動できます。これが内部ソリューションである場合、多くの場合、組織は開発環境やテスト環境などの時間に敏感でないプロセスを実行し、必要に応じて本番環境のリカバリのために脇に置きます。この戦略を採用する場合、O / Sレベル、ハードウェアの違い、容量の違いなどの問題が回復を妨げたり遅らせたりしないように、2つの環境を可能な限り同一に保つことが重要です。
リカバリサイトの戦略テクノロジのリカバリを完了する必要があるまでの組織のダウンタイムに応じて、テクノロジ環境用に選択されるリカバリ戦略は次のいずれかになります。

デュアルデータセンター-この戦略は、組織に悪影響を与えることなくダウンタイムを受け入れることができないアプリケーションに採用されています。アプリケーションは、地理的に分散した2つのデータセンターに分割され、2つのセンター間で負荷分散されるか、2つのセンター間でホットスワップされます。存続するデータセンターには、いずれの場合も本番環境の全負荷を処理するのに十分なヘッドルームが必要です。
外部ホットサイト-この戦略では、フロアに機器が待機していますが、環境は
回復のために再構築されました。これらは、リカバリサービスプロバイダーを通じて契約されたサービスです。また、
回避するために、2つの環境を可能な限り同一に保つことが重要です。
O / Sレベル、ハードウェアの違い、容量の違いなどの問題による防止または
回復を遅らせる。ホットサイトベンダーは、最も一般的に使用されるハードウェアとソフトウェアを使用する傾向があります
サイトを利用するために最も多くの顧客を引き付ける製品。ユニークな機器または
ソフトウェアは通常、災害時または災害時に組織が提供する必要があります。
事前にそこに保管されています。
ウォームサイト-リースまたはレンタルされた施設で、通常は一部の機器で部分的に構成されていますが、
実際のコンピューターではありません。通常、すべての冷却、ケーブル接続、およびネットワークが適切に配置されます。
リカバリに対応しますが、実際のサーバー、メインフレームなど、機器は
災害時のサイト。
コールドサイト-コールドサイトは、フロアにテクノロジーがないシェルまたは空のデータセンタースペースです。全て
技術は災害時に購入または取得する必要があります。
この質問に使用される参照：
Hernandez CISSP、Steven（2012-12-21）。CISSP CBK、第3版の公式（ISC）2ガイド（ISC）2 Press）Kindle Locations 21265-21291）。AuerbachPublications。キンドル版。

最新問題: **180**
コントロールの復元に関係するコントロールのタイプはどれですか？
A. 補正コントロール
B. 修正コントロール
C. 探偵コントロール
D. 予防管理
Answer: B (メーッセージを残す**)**
説明/参照：
Explanation:
修正制御は、インシデントが発生した後にシステムを復元するために使用されます。
セキュリティ制御のさまざまな機能は、予防、検出、修正、抑止、回復、および補償です。
6つの異なる制御機能は次のとおりです。

抑止力：潜在的な攻撃者を思いとどまらせることを目的としています
- 予防：インシデントの発生を回避することを目的としています
- 修正：インシデントが発生した後にコンポーネントまたはシステムを修正します
- リカバリ：環境を通常の操作に戻すことを目的としています
- 探偵：事件の活動と潜在的に侵入者を特定するのに役立ちます
- 補償：制御の代替手段を提供する制御

不正解：
A：補償コントロールは、コントロールの代替手段を提供します。インシデント後にシステムを復元するために使用されることはありません。
C：探偵コントロールは、有害な出来事を発見するために使用されます。インシデント後にシステムを復元するために使用されることはありません。
D：インシデントの発生を回避するために予防管理が使用されます。インシデント後にシステムを復元するために使用されることはありません。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、2013、p。30

最新問題**: 181**
証人の五感で集めた情報に基づいた口頭での証言を通じて、特定の行為を証明または反証するのは次のうちどれですか？
A. 直接的な証拠。
B. 状況証拠。
C. 決定的な証拠。
D. 裏付けとなる証拠。
Answer: (解答を表示する**)**
説明/参照：
Explanation:
直接的な証拠はそれ自体で事実を証明することができ、参照するためのバックアップ情報を必要としません。直接的な証拠は、多くの場合、証人の五感から収集された情報に基づいています。
不正解：
B：状況証拠は中間的な事実を証明することができますが、それ自体では直接的な事実を証明することはできません。次に、中間ファクトを使用して、別のファクトの存在を推測または想定できます。
C：証人の五感からは、決定的な証拠は収集されていません。決定的な証拠は反駁できないものであり、矛盾することはありません。決定的な証拠はそれ自体が非常に強力であり、確証を必要としません。
D：裏付けとなる証拠は、アイデアやポイントを証明するために使用される証拠を裏付けるものです。それは自立できないので、特定の行為を反証することはできません。
参照：

Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、New York、2013、p。1055

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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**
Bell-LaPadulaモデルの単純なセキュリティ（ss）プロパティはどういう意味ですか？
A. 読み上げなし
B. 書き留めなし
C. 読み上げなし
D. 書き込みなし
Answer: (解答を表示する**)**
Bell-LaPadulaアクセス制御モデルのss（単純なセキュリティ）プロパティは、感度レベルの高いオブジェクトから感度レベルの低いサブジェクトによる情報の読み取りは許可されない（読み取りなし）ことを示しています。
出典：KRUTZ、Ronald L.＆VINES、Russel D.、CISSP準備ガイド：マスタリングコンピュータセキュリティの10のドメイン、John Wiley＆Sons、2001年、第5章：セキュリティアーキテクチャとモデル（202ページ）。

最新問題: **183**
通信チャネルが任意の数の可変ビットレートデジタルチャネルまたはデータストリームに分割されるデータを多重化する方法は、次のうちどれですか。この方法では、送信する情報を持つ物理チャネルに帯域幅を動的に割り当てますか？
A. 時分割多重
B. 非同期時分割多重
C. 統計多重化
D. 周波数分割多重
Answer: C (メーッセージを残す**)**
統計多重化は、通信リンク共有の一種であり、
動的帯域幅割り当て（DBA）。統計多重化では、通信チャネルは
任意の数の可変ビットレートデジタルチャネルまたはデータストリームに分割されます。リンク共有は、転送されるデータストリームの瞬間的なトラフィック需要に適応します
各チャネルで。これは、一般的なリンクの固定共有を作成する代わりの方法です。
時分割多重（TDM）および周波数分割多重（FDM）。実行時
正しくは、統計多重化は、統計と呼ばれるリンク使用率の改善を提供できます

多重化ゲイン。
一般に、データを多重化する方法には次のものがあります。
時分割多重（TDM）：各データチャネルからの情報に帯域幅が割り当てられます
送信するデータがあるかどうかに関係なく、事前に割り当てられたタイムスロットに基づきます。時分割多重化は主にデジタル信号に使用されますが、2つ以上の信号またはビットストリームが転送され、1つの通信チャネルにサブチャネルとして同時に表示されるが、チャネルを物理的に交代させるアナログ多重化に適用できます。時間領域は、サブチャネルごとに1つずつ、固定長の複数の繰り返しタイムスロットに分割されます。サブチャネル1のサンプルバイトまたはデータブロックは、タイムスロット1、サブチャネル2、タイムスロット2などで送信されます。1つのTDMフレームは、サブチャネルごとに1つのタイムスロットと同期チャネル、場合によってはエラー修正チャネルで構成されます。同期前。最後のサブチャネル、エラー訂正、および同期の後、
非同期時分割多重（ATDM）データチャネルからの情報には、動的に割り当てられたタイムスロットを介して、必要に応じて帯域幅が割り当てられます。ATMは、回線交換ネットワークとパケット交換ネットワークの両方に類似した機能を提供します。ATMは、非同期時分割多重化を使用し、データをセルと呼ばれる小さな固定サイズのパケット（ISO-OSIフレーム）にエンコードします。これは、可変サイズのパケットとフレームを使用するインターネットプロトコルやイーサネットなどのアプローチとは異なります。ATMは、実際のデータ交換を開始する前に2つのエンドポイント間に仮想回線を確立する必要があるコネクション型モデルを使用します。これらの仮想回線は、「永続的」、つまり通常はサービスプロバイダーによって事前構成されている専用接続、または「スイッチド」、つまり
周波数分割多重（FDM）：各データチャネルからの情報には、トラフィックの信号周波数に基づいて帯域幅が割り当てられます。電気通信では、周波数分割多重（FDM）は、通信媒体で利用可能な全帯域幅を一連の重複しない周波数サブバンドに分割する手法であり、各サブバンドは個別の信号を伝送するために使用されます。これにより、無線スペクトル、ケーブル、光ファイバーなどの単一の伝送媒体を多くの信号で共有できます。
この質問に使用される参照：http://en.wikipedia.org/wiki/Statistical_multiplexingおよびhttp://en.wikipedia.org/wiki/Frequency_division_multiplexing and Information Systems Audit and Control Association、Certified Information Systems Auditor 2002 review manual、Chapter 3：技術インフラストラクチャと運用方法（114ページ）。

最新問題: **184**
攻撃者がICMPECHOブロードキャストパケットの送信元IPアドレスをスプーフィングして、被害者のシステムから発信されたように見せかけ、REPLYパケットで溢れさせる攻撃とは何ですか？
A. SYNフラッド攻撃
B. スマーフ攻撃
C. PingofDeath攻撃
D. サービス拒否（DOS）攻撃
Answer: B (メーッセージを残す**)**

被害者のシステムへのサービス拒否を引き起こす可能性がありますが、このタイプの攻撃はSmurf攻撃です。SYNフラッド攻撃は、被害者のシステムに多数の偽の通信ソケットを設定することにより、システムのすべてのリソースを使い果たします。Ping of Death攻撃は、有効な最大長（65535オクテット）を超えるIPパケットを送信することによって実行されます。出典：HARRIS、ション、オールインワンCISSP認定試験ガイド、McGraw-Hill / Osborne、2002年、第11章：アプリケーションとシステムの開発（789ページ）。

最新問題: **185**
ISO / IEC 27001：2005は、次の規格です。
A. 情報セキュリティマネジメントシステム
B. 基本的なセキュリティ対策の実施と認証
C. 暗号化アルゴリズムの検証のための評価基準
D. 公開鍵インフラストラクチャの認証
Answer: A (メーッセージを残す**)**
http://www.27000.org/index.htmにあるISO27000ディレクトリには、ISO27000シリーズの優れたカバレッジがあります。以下のテキストは彼らのウェブサイトから抽出されました。
ベリンダが言及しているように、ISO27001規格は認証管理基準です。
ISO27002が実際の規格です。ISO 27002は、名前が変更される前はISO17799と呼ばれていました。
ISO 27001（ISO27001）の概要
ISO 27001規格は、2005年10月に公開され、基本的に古いものに取って代わりました。
BS7799-2標準。情報セキュリティであるISMSの仕様です
マネジメントシステム。BS7799自体は長年の標準であり、90年代に実践規範として最初に公開されました。これが成熟するにつれて、管理システムをカバーするための2番目の部分が出現しました。これに対して認証が付与されます。今日、世界中で1,000を超える証明書が発行されています。
ISO 27001は、BS7799-2のコンテンツを強化し、他の標準と調和させました。BS7799認証からISO27001認証に変換するためのスキームがさまざまな認証機関によって導入されています。
この規格自体の目的は、「情報セキュリティを確立、実装、運用、監視、レビュー、維持、および改善するためのモデルを提供することです。
管理システム」。その採用に関しては、これは戦略的な決定である必要があります。さらに、「組織のISMSの設計と実装は、組織のニーズと目的、セキュリティ要件、採用されているプロセス、および組織の規模と構造に影響されます。」
この規格では、「プロセスアプローチ」を「組織内のプロセスシステムの適用と、これらのプロセスの識別と相互作用、およびそれらの管理」と定義しています。PDCA、Plan-Do-Check-Actモデルを使用してプロセスを構造化し、OECDガイドライン（oecd.orgを参照）に定められた原則を反映しています。
ISO27001の内容
標準のコンテンツセクションは次のとおりです。
経営責任

内部監査
ISMSの改善
附属書A-統制の目的と統制
附属書B-OECDの原則とこの国際規格
附属書C-ISO9001、ISO14001とこの規格との対応
ISO 27002 (ISO27002)の概要
ISO 27002規格は、ISO 17799規格の名前を変更したものであり、情報セキュリティの実践規範です。それは基本的に、ISO 27001内で提供されるガイダンスに従って、理論的には実装される可能性のある何百もの潜在的な制御と制御メカニズムの概要を示しています。
この規格は、 組織内の情報セキュリティ管理を開始、実装、維持、および改善するための確立されたガイドラインと一般原則」です。規格に記載されている実際の統制は、正式なリスク評価によって特定された特定の要件に対処することを目的としています。この標準は、 組織のセキュリティ標準と効果的なセキュリティ管理手法の開発、および組織間の活動への信頼の構築を支援する」ためのガイドを提供することも目的としています。
この規格の基礎は、もともと英国政府によって発行された文書であり、1995年にBSIによって BS7799として再発行されたときに、標準の 適切な」ものになりました。の
2000年にISO17799として再発行されました。2005年に新しいバージョンのISO27001とともに、この2つのドキュメントが一緒に使用されることを目的としています。。
この規格に関するISOの将来の計画は、主に業界固有のバージョン たとえば、医療部門、製造業など)の開発と公開に焦点を合わせています。これは時間のかかるプロセスであるため、新しい標準が表示されるまでに時間がかかることに注意してください
ISO17799/27002の内容
コンテンツセクションは次のとおりです。
構造
リスク評価と治療
セキュリティポリシー
情報セキュリティの組織
資産運用管理
人的資源のセキュリティ
物理的セキュリティ
コミュニケーションと運用管理
アクセス制御
情報システムの取得、開発、保守
情報セキュリティインシデント管理
事業継続性
コンプライアンス
http://www.iso.org/iso/catalogue_detail?csnumber=42103
と
http://www.27000.org/index.htmのISO27000ディレクトリ

最新問題: **186**
電気システムは、コンピューター操作の生命線です。清潔で安定した供給の継続
適切な人的環境を維持し、データ操作を維持するには、電力が必要です。次のうち、電力システムを脅かす可能性のある要素ではないものはどれですか？
A. 過渡ノイズ
B. 障害のある地面
C. 電圧低下
D. UPS
Answer: (解答を表示する**)**
無停電電源装置、無停電電源装置、UPSまたは
バッテリー/フライホイールバックアップは、次の場合に負荷に緊急電力を供給する電気装置です。
入力電源（通常は主電源）に障害が発生します。UPSは補助または緊急事態とは異なります
入力からほぼ瞬時に保護するという点で、電力システムまたは予備発電機
バッテリーまたはフライホイールに蓄えられたエネルギーを供給することによる停電。バッテリー上のランタイム
ほとんどの無停電電源装置は比較的短いですが（わずか数分）、起動するには十分です
待機電源または保護された機器を適切にシャットダウンします。
UPSは通常、コンピューター、データセンター、通信機器などを保護するために使用されます
予期しない停電が怪我、死亡、深刻な原因となる可能性のある電気機器
ビジネスの混乱またはデータの損失。
UPSの主な役割は、入力電源に障害が発生したときに短期間の電力を供給することです。
ただし、ほとんどのUPSユニットは、一般的な商用電源をさまざまな程度で修正することもできます。
問題：
電圧スパイクまたは持続的な過電圧
入力電圧の瞬間的または持続的な低下。
高周波過渡または発振として定義されるノイズ。通常、近くからラインに注入されます。
装置。
主電源周波数の不安定性。
高調波歪み :で予想される理想的な正弦波形からの逸脱として定義されます。
ライン。
ノート：
一部の組織は常にUPSを使い果たしています。もちろん、そのような場合、オンラインUPSの場合
失敗し、冗長性について考えていなかった場合、それは支援する代わりに失敗に寄与する可能性があります
停電を避けるため。スタンバイUPSが問題を引き起こす可能性があることが、数人のクイズ受験者から報告されました
同じように。私は完全に同意しますが、これは標準よりも例外です。対策、

セーフガード、または適切に展開または維持されていないコントロールは、代わりにリスクをもたらす可能性があります
それらの影響を最小限に抑えるか、それらを防ぎます。繰り返しになりますが、質問は見ようとはしていません
考えられるすべての問題と状況、あなたは質問の文脈の中にとどまらなければなりません、あなたは見ます
4つの選択肢を選択し、提示された質問に従ってどれが最適かを確認します。を見て
この質問とともに提示された4つの選択肢から、UPSは電力の問題を引き起こす可能性が最も低いことは間違いありません。
この質問に使用される参照 :http ://en.wikipedia.org/wiki/Uninterruptible_power_supply

最新問題: **187**
データ侵害による個人情報 PII)の損失を最小限に抑えるには、どのセキュリティアプローチが最適ですか？
A. 転送中のデータのエンドツーエンドのデータ暗号化
B. 潜在的な脆弱性の継続的な監視
C. 強力な違反通知プロセス
D. 個人の機密データの限定的な収集
Answer: D (メーッセージを残す**)**
セクション :セキュリティアーキテクチャとエンジニアリング

最新問題: **188**
次のうち、公開鍵暗号システムのプロパティではないものはどれですか？
 Pは秘密鍵を表し、Qは公開鍵を表し、Mは
プレーンテキストメッセージ。）
A. PとQは、特定のキー値から生成するのは困難です。
B. P [Q M)] = M
C. Q [P M)] = M
D. QからPを導出することは計算上実行不可能です。
Answer: (解答を表示する**)**
答えは、秘密鍵と公開鍵が計算される最初の計算を指します。この方向の計算は比較的簡単です。回答 Q[P M)] =M」および P[Q M)] = M」は、秘密鍵で暗号化された平文メッセージを公開鍵で復号化できるという、公開鍵暗号の真の特性を示しています。およびその逆。回答 QからPを導出することは計算上実行不可能です」は、公開鍵から秘密鍵を導出することは計算上実行不可能であると述べています。明らかに、これは公開鍵暗号の重要な特性です。

最新問題: **189**
次のうち、米国国防総省のために国家コンピュータセキュリティセンター NCSC)によって開発されたものはどれですか？
A. TCSEC

B. ITSEC
C. DIACAP
D. NIACAP
Answer: A (メーッセージを残す)
説明/参照：
Explanation:
信頼できるコンピューターシステム評価基準（TCSEC）は、コンピューターシステムに組み込まれているコンピューターセキュリティ制御の有効性を評価するための基本的な要件を設定する米国国防総省（DoD）の標準です。TCSECは、機密情報または機密情報の処理、保存、および取得を検討しているコンピューターシステムを評価、分類、および選択するために使用されました。
オレンジブックと呼ばれることが多いTCSECは、DoDRainbowシリーズの出版物の目玉です。1983年に国家安全保障局の機関であるNationalComputerSecurity Center（NCSC）によって最初に発行され、その後1985年に更新されました。TCSECは、2005年に最初に公開されたCommonCriteria国際規格に置き換えられました。
不正解：
B：情報技術セキュリティ評価基準（ITSEC）は、多くのヨーロッパ諸国によるコンピュータシステムおよび製品のセキュリティ属性を評価するための単一の標準を確立する最初の試みでした。これは質問で説明されていることではありません。
C：DoD情報保証認証および認定プロセス（DIACAP）は、米国国防総省（DoD）のプロセスであり、企業や組織が情報システム（IS）にリスク管理を適用することを保証します。これは質問で説明されていることではありません。
D：国家情報保証認証および認定プロセス（NIACAP）は、米国を扱うコンピューターおよび電気通信システムの認証および認定のための最低限の標準プロセスです。これは、質問で説明されているものではありません。
参照：
https://en.wikipedia.org/wiki/Trusted_Computer_System_Evaluation_Criteria Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、New York、2013、p。399

最新問題**: 190**
フェイルオーバーという用語は、次のことを指します。
A. フェイルソフトシステム。
B. 制御された方法で処理を終了します。
C. 回復力。
D. 複製のホットバックアップコンポーネントに切り替えます。
Answer: D (メーッセージを残す)
正解は「重複したホットバックアップコンポーネントへの切り替え」です。フェイルオーバーとは、プライマリシステムとの重複状態を維持するホットバックアップシステムに切り替えることを意味します。回答「制御された方法で処理を終了する」はフェイルセーフを指し、回答は復元力とフェイルソフトシステムはフェイルソフトを指します。

最新問題: **191**
リスク管理を最もよく定義するものは何ですか？
A. リスクを排除するプロセス
B. リスクを評価するプロセス
C. リスクを許容レベルまで低減するプロセス
D. リスクを移転するプロセス
Answer: (解答を表示する**)**
これがリスク管理の基本的なプロセスです。
リスクとは、損傷が発生する可能性と、発生した場合のそのような損傷の影響です。情報リスク管理（IRM）は、リスクを特定して評価し、許容可能なレベルまでリスクを低減し、そのレベルを維持するための適切なメカニズムを実装するプロセスです。100%安全な環境というものはありません。すべての環境には、ある程度の脆弱性と脅威があります。
このスキルは、これらの脅威を特定し、実際に発生する可能性とそれらが引き起こす可能性のある損害を評価し、組織が許容できると特定したレベルまで環境内のリスクの全体的なレベルを下げるための適切な手順を実行することです。
適切なリスク管理には、上級管理職からの強いコミットメント、組織の使命をサポートする文書化されたプロセス、情報リスク管理（IRM）ポリシー、および委任されたIRMチームが必要です。会社の許容可能なリスクレベルを特定したら、情報リスク管理ポリシーを作成する必要があります。
IRMポリシーは、組織の全体的なリスク管理ポリシーのサブセットである必要があります（企業へのリスクには、情報セキュリティの問題以上のものが含まれます）。組織のセキュリティポリシーにマッピングする必要があります。これにより、許容可能なリスクと組織全体のセキュリティの役割が示されます。IRMポリシーはリスク管理に重点を置いていますが、セキュリティポリシーは非常に高レベルであり、セキュリティのすべての側面に対応しています。IRMポリシーは、次の項目に対処する必要があります。
IRMチームの目的
会社が受け入れるリスクのレベルと、許容できるリスクと見なされるもの（前の記事で定義）
リスク特定の正式なプロセス
IRMポリシーと組織の戦略的計画プロセスとの関係
IRMに該当する責任とそれらを遂行する役割
内部統制へのリスクのマッピング
リスク分析に応じてスタッフの行動とリソースの割り当てを変更するためのアプローチ
パフォーマンス目標と予算へのリスクのマッピング
コントロールの有効性を監視するための主要な指標
ションハリスは、以下のリスク管理プロセスの10,000フィートのビューを提供します。
企業が対処しなければならない大きな問題は、「十分なセキュリティとは何か」です。これは、「許容できるリスクレベルはどれくらいですか？」と言い換えることができます。これらの2つの質問には逆の関係があります。必要なベースラインリスクレベルを知らない限り、何が十分なセキュリティを構成するのかを知ることはできません。

企業全体で許容できるリスクレベルを設定するには、いくつかのことを調査して理解する必要があります。企業は、連邦および州の法的要件、規制要件、ビジネスの推進要因と目的を理解し、リスクと脅威の分析を実行する必要があります。（正式なリスク分析プロセスについては後の記事で詳しく説明しますが、今のところは幅広いアプローチを取ります。）次に、これらの調査結果を使用して、会社の許容可能なリスクレベルを定義し、セキュリティポリシーで概説します。標準、ガイドライン、および手順。
エンタープライズリスク管理にはさまざまな方法論がありますが、リスク分析のコアコンポーネントは次のもので構成されています。
会社の資産を特定する
各アセットに値を割り当てます
各資産の脆弱性と関連する脅威を特定する
識別された資産のリスクを計算します
これらの手順が完了すると、リスク分析チームは、計算されたリスクを軽減するために必要な対策を特定し、これらの対策の費用便益分析を実行して、その結果を上級管理職に報告できます。
情報セキュリティを見ると、企業が認識し、適切に対処する必要のあるリスクにはいくつかの種類があります。次の項目は、主要なカテゴリに触れています。
*物理的損傷火災、水、破壊行為、停電、自然災害
*人間の相互作用生産性を混乱させる可能性のある偶発的または意図的な行動または不作為
*機器の誤動作システムおよび周辺機器の故障
*内部および外部の攻撃ハッキング、クラッキング、および攻撃
*データの悪用企業秘密の共有、詐欺、スパイ、盗難
*データの損失破壊的な手段による意図的または意図的でない情報の損失
*アプリケーションエラー計算エラー、入力エラー、およびバッファオーバーフロー
次の答えは正しくありません。
リスクを完全に排除することはできないため、リスクを排除するプロセスは最善の答えではありません。
リスクを評価するプロセスも最善の答えではありません。
リスクを移転するプロセスも最善の答えではなく、リスク分析が実行された後にリスクを処理する方法の1つです。
参照：
ション・ハリス、AIO v3、第3章：セキュリティ管理の実践、ページ：66-68および
http://searchsecurity.techtarget.com/tip/Understanding-risk

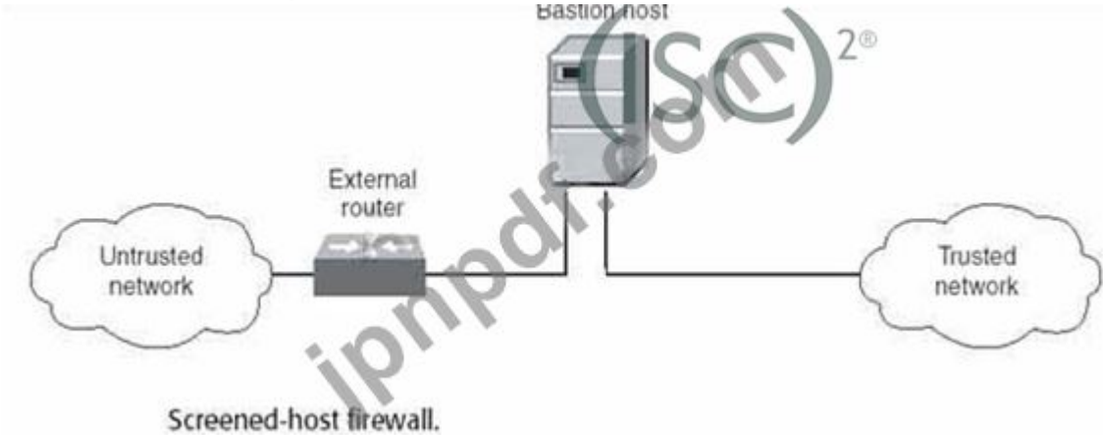
最新問題: **192**
情報分類の目的は
A. さまざまな保護対策を適用します。
B. セキュリティラベルに必要なパラメータを定義します。
C. 職務の分離を確実にします。
D. アクセス制御を割り当てます。
Answer: A (メーッセージを残す**)**

最新問題: **193**
Rijndael暗号化アルゴリズムの最大許容キーサイズはいくつですか？
A. 128ビット
B. 192ビット
C. 256ビット
D. 512ビット
Answer: C (メーッセージを残す**)**
DESの代わりにAdvancedEncryptionStandard（AES）として選択されたRijndaelアルゴリズムは、128、192、または256ビットとして個別に選択できる可変ブロック長とキー長を持つ反復ブロック暗号として分類できます。
以下に、AESとRijndaelの違いの概要を示します。
AESは、FIPS 197で定義されている高度な暗号化標準です。これは、Rijndaelとは異なる方法で実装されています。
FIPS-197は、AESではブロックサイズが常に128ビットである必要があり、キーサイズが128、192、または256ビットのいずれかであることを指定しています。したがって、AES-128、AES-192、およびAES-256は実際には次のとおりです。
キーサイズ（ビット）ラウンド数
ブロックサイズ（ビット）
AES-128
12810ラウンド
1 28
AES-192
19212ラウンド
1 28
AES-256
25614ラウンド
1 28
いくつかの本は「最大9ラウンドは128ビットキーで行われる」と言うでしょう。最初のラウンドであるラウンドゼロを含める必要があるため、実際には10ラウンドです。
対照的に、Rijndael仕様自体は、最小128ビットと最大256ビットの両方で32ビットの倍数のブロックおよびキーサイズで指定されます。
この質問に使用される参照：
KRUTZ、Ronald L.＆VINES、Russel D.、CISSP準備ガイド：10をマスターする Domains of Computer Security、John Wiley＆Sons、2001年、第4章：暗号化（ページ153）。
と
FIPS 197
と
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

最新問題: **194**
次のうち、暗号化ハッシュの特徴ではないものはどれですか
関数、H ⑯、ここでmは、によってハッシュされているメッセージを示します。
関数H？
A. H ⑯は一方向性関数です。
B. H ⑯は、任意のmに対して計算するのが困難です。
C. 出力は固定長です。
D. H ⑯は衝突がありません。
Answer: (解答を表示する**)**
暗号化ハッシュ関数の場合、H ⑯は比較的簡単に計算できます。
与えられたmに対して。
*回答 Ｈ ⑯は衝突がない」は、優れた暗号化ハッシュ関数の特徴です。衝突がないということは、H Ⓜ= Zを生成する特定のメッセージMに対して、別のメッセージを見つけることが計算上不可能であることを意味します。メッセージM1、H Ⓜ1）=Z。
*回答 出力は固定長です」はの定義の一部です
入力メッセージの長さに依存しない固定長の結果を生成するため、ハッシュ関数。この特性は、通常はハッシュよりもはるかに長いメッセージ全体ではなく、メッセージに固有の特性である固定長のハッシュに署名を適用できるため、デジタル署名の生成に役立ちます。
*回答 Ｈ ⑯は一方向性関数です」は、一方向性関数を反転することが困難または不可能であるという点で、 Ｈ ⑯は任意のmに対して計算するのが難しい」という回答に関連しています。これは、ハッシュ関数H Ⓜ= Zの場合、プロセスを逆にしてMを見つけることは計算上実行不可能であることを意味します。
ハッシュZと関数H。

最新問題: **195**
2つのネットワークカードと1つのファイアウォールアーキテクチャを採用しているのはどのタイプのファイアウォールアーキテクチャですか。
シングルスクリーニングルーター？
A. デュアルホームホストファイアウォール
B. アプリケーションレベルのプロキシサーバー
C. スクリーニングされたサブネットファイアウォール
D. スクリーニングされたホストファイアウォール
Answer: (解答を表示する**)**
デュアルホームホストと同様に、スクリーニングされたホストファイアウォールは、2枚のネットワークカードを使用して信頼できるネットワークと信頼できないネットワークに接続しますが、ホストと信頼できないネットワークの間にスクリーニングルーターを追加します。
*デュアルホームホストには2つのNICがありますが、必ずしもスクリーニングルーターである必要はありません。

*screened-subnetファイアウォールも2つのNICを使用しますが、ホストに2つのスクリーニングルーターがあります。



独自のネットワークセグメントでプロキシサーバーとして機能します。1つのスクリーニングルーターはネットワークのローカルトラフィックを制御し、もう1つのルーターは着信および発信インターネットトラフィックを監視および制御します。
*アプリケーションレベルのプロキシは、この質問とは関係ありません。出典：LarsKlanderによるHackerProof（Jamsa Press、1997）。

最新問題: **196**
NOPの長い文字列とそれに続くコマンドを含むパケットは、通常、何を示していますか？
A. シンスキャン
B. ハーフポートスキャン
C. バッファオーバーフロー
D. ネットワークのブロードキャストアドレス宛てのパケット
Answer: C (メーッセージを残す**)**
参考資料 「このペーパーは、バッファオーバーフローエクスプロイトを作成するための実用的なアプローチが必要なユーザーを対象としています。タイトルにあるように、このテキストでは、これらのエクスプロイトをPerlで作成する方法を説明します。.....バッファを作成する理由は次のとおりです。最初に多くのNOPがあり、次にシェルコード（この例では/ bin / shを実行します）、最後にESP+オフセット値があります。」http://hackersplayground.org/papers/perl-buffer.txt

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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: **197**

アプリケーションの設計レビューが完了し、リリースの準備が整いました。アプリケーションの整合性を保証するために、組織はどのような手法を使用する必要がありますか？
A. アプリケーション認証
B. 入力検証
C. デジタル署名
D. デバイスの暗号化
Answer: C (メーッセージを残す**)**
セクション :ソフトウェア開発のセキュリティ
説明/参照：

最新問題**: 198**
このベースラインは、許可される特定のエラーまたはミスの特定のしきい値と、疑わしいと見なされる前に発生する可能性のあるこれらの発生の量を設定しますか？
A. チェックポイントレベル
B. 天井レベル
C. クリッピングレベル
D. しきい値レベル
Answer: C (メーッセージを残す**)**
組織は通常、特定の種類、数、またはパターンの違反を許しているため、分析のためにこのデータを収集する前に、事前に決定された数のユーザーエラーを許可します。高度な統計計算能力がなければ、すべての違反を追跡しようとする組織は、そのようなデータの膨大な量を管理することができません。違反リストを有効にするには、クリッピングレベルを確立する必要があります。クリッピングレベルは、通常のユーザーエラーである可能性のある違反アクティビティのベースラインを確立します。このベースラインを超えた後にのみ、違反レコードが作成されます。このソリューションは、中小規模の設置に特に効果的です。大規模なコンピューティング機能を備えた組織は、多くの場合、すべての違反を追跡し、統計ルーチンを使用して軽微な違反を排除します（たとえば、パスワードを忘れたり、パスワードを数回間違えたりします）。
追跡されている違反の数が管理不能になった場合、問題を修正するための最初のステップは、状態が発生した理由を分析することです。ユーザーは、コンピューターリソースとの対話方法を理解していますか？ルールに従うのは難しすぎますか？違反の追跡と分析は、組織が徹底的でありながら使用可能な制御を開発するのを支援する上で貴重なツールになる可能性があります。これらが実施され、重大な違反を正確に反映する記録が作成されると、追跡と分析が最初の防衛線になります。この手順では、大きな損傷が発生する前に、場合によっては実行者を捕まえるのに十分早い段階で侵入が発見されます。さらに、事業の保護と保全が強化されます。
次の答えは正しくありません。
提示された他のすべての選択肢は、単に中傷者でした。
この質問には、次の参照が使用されました。
情報セキュリティマネジメントハンドブック

最新問題**: 199**

従来の制御フレームワークと比較して、DevOpsプラクティスを採用する場合、セキュリティ上の重要な課題と見なすことができるのは次のうちどれですか？
A. ロギング、アラート、およびセキュリティメトリックの標準化された構成。
B. 設計プロセスの最後に、土壇場での手動監査とレビューを実行するためのセキュリティチームの可用性。
C. セキュリティ上の欠陥が見つかった場合にパッチがリリースされるまでの時間に関するサービスレベルアグリーメント（SLA）の達成。
D. 職務の分離を維持します。
Answer: D (メーッセージを残す)

最新問題: **200**
質問に答えるには、以下の情報を参照してください。
マルチレベルセキュリティ（MLS）システムでは、次の機密ラベルが機密レベルの増加に使用されます：制限付き、機密、秘密、極秘。表Aに4人のユーザーのクリアランスレベルを示し、表Bに4つの異なるファイルのセキュリティクラスを示します。

Table A

User	Clearance Level
A	Restricted
B	Confidential
C	Secret
D	Top Secret

Table B

Files	Security Class
1	Restricted
2	Confidential
3	Secret
4	Top Secret

jpnpdf.com (ISC)

星のプロパティ（*プロパティ）に応じて、次のうち正しいものはどれですか？
A. ユーザーAはファイル1に書き込むことができます
B. ユーザーCはファイル1に書き込むことができます
C. ユーザーDはファイル1に書き込むことができます
D. ユーザーBはファイル1に書き込むことができます
Answer: A (メーッセージを残す)

最新問題: **201**
あなたは、クライアントのネットワークで侵入テストを実行する必要があるセキュリティコンサルタントです。ペネトレーションテストでは、ファイアウォールなどのネットワーク制限を回避するために、侵害されたシステムを使用してネットワーク上の他のシステムを攻撃する必要があります。このシナリオでは、どの方法を使用しますか。
A. ブラックボックス方式
B. ピボット方式
C. ホワイトボックス方式。
D. グレイボックス法

Answer: (解答を表示する**)**
ピボットとは、侵入テスターが使用する方法で、侵害されたシステムを使用して同じネットワーク上の他のシステムを攻撃し、すべてのマシンへの直接アクセスを禁止する可能性のあるファイアウォール構成などの制限を回避します。たとえば、攻撃者が企業ネットワーク上のWebサーバーを侵害した場合、攻撃者は侵害されたWebサーバーを使用してネットワーク上の他のシステムを攻撃する可能性があります。これらのタイプの攻撃は、しばしば多層攻撃と呼ばれます。ピボットはアイランドホッピングとも呼ばれます。
ピボットはさらにプロキシピボットとVPNピボットに区別できます。プロキシピボットは一般に、マシン上のプロキシペイロードを使用して、侵害されたターゲットを介してトラフィックを誘導し、このコンピューターから攻撃を開始する方法を表します。[1] このタイプのピボットは、プロキシでサポートされている特定のTCPおよびUDPポートに制限されています。VPNピボットを使用すると、攻撃者は暗号化されたレイヤー2トンネルを侵入先のマシンに作成して、そのターゲットマシンを介してネットワークトラフィックをルーティングできます。たとえば、侵入先のマシンを介して内部ネットワークで脆弱性スキャンを実行し、攻撃者に次のような完全なネットワークアクセスを効果的に提供できます。彼らがファイアウォールの後ろにいた場合。
通常、ピボットを有効にするプロキシまたはVPNアプリケーションは、エクスプロイトのペイロード（ソフトウェア）としてターゲットコンピューター上で実行されます。
次の答えは正しくありません。
ブラックボックス方式
ブラックボックステストは、アプリケーションの機能を次のようにテストするソフトウェアテストの方法です。
その内部構造または動作とは対照的です（ホワイトボックステストを参照）。の特定の知識
アプリケーションのコード/内部構造およびプログラミングの一般的な知識は必要ありません。The
テスターは、ソフトウェアが何をすることになっているのかだけを知っていますが、どのように、つまり彼が
特定の入力、彼は特定の出力を取得します。出力がどのように生成されたかを意識せずに
最初の場所。テストケースは、仕様と要件、つまりアプリケーションが何であるかを中心に構築されています
することになっています。仕様を含むソフトウェアの外部記述を使用します。
要件、およびテストケースを導出するための設計。これらのテストは、機能的または非機能的である可能性があります。
通常は機能しますが。テスト設計者は、有効な入力と無効な入力を選択し、
正しい出力。テストオブジェクトの内部構造に関する知識はありません。
ペネトレーションテストの場合、ターゲットについての知識がないことを意味します。IPのみを取得できます
アドレスまたはドメイン名とその非常に限られた量の知識からあなたが試みなければならない
あなたができるすべてを見つけてください。
ホワイトボックス法

ペネトレーションテストでは、ホワイトボックステストとは、ホワイトハットハッカーが満員になる方法を指します。
攻撃されているシステムに関する知識。ホワイトボックス侵入テストの目標は、
ターゲットシステムに対するある程度の知識と、場合によっては基本的な資格情報を持っている悪意のあるインサイダー。
グレイボックス法
グレーボックステストは、ホワイトボックステストとブラックボックステストを組み合わせたものです。このテストの目的は
不適切な構造またはアプリケーションの不適切な使用に起因する欠陥がある場合は、それを検索します。
CEHのコンテキストでは、これは企業ネットワークの内部テストも意味します。
この質問を作成するために、次の参照が使用されました。
https://en.wikipedia.org/wiki/Exploit_%28computer_security%29#Pivoting
https://en.wikipedia.org/wiki/Black-box_testing
Hernandez CISSP、Steven（2012-12-21）。CISSP CBK、第3版の公式（ISC）2ガイド（（ISC）2 Press）K(indle Locations 4656-4657）。AuerbachPublications。キンドル版。

最新問題: **202**
Kerberosに関する次の説明のうち正しいものはどれですか？
A. Kerberosは可用性に対応していません
B. Kerberosは整合性に対応していません
C. Kerberosは対称鍵を使用しません
D. Kerberosは情報の機密性に対処できません
Answer: A (メーッセージを残す**)**
質問はTRUEステートメントを要求することであり、唯一の正しいステートメントは「Kerberosは可用性に対応していません」です。
Kerberosは、情報の機密性と整合性に対応しています。可用性については直接言及していません。
出典：KRUTZ、Ronald L.＆VINES、Russel D.、CISSP準備ガイド：マスタリング
コンピュータセキュリティの10のドメイン、John Wiley＆Sons、2001年、第2章：アクセス制御システム（42ページ）。

最新問題: **203**
ネットワークセキュリティエンジニアは、セキュリティソリューションがトラフィックを分析して、プロトコル操作やさまざまな種類の一般的な攻撃がないかどうかを確認する必要があります。さらに、すべてのURL（Uniform Resource Locator）トラフィックを検査し、ユーザーが不適切なWebサイトを閲覧できないようにする必要があります。管理者がトラフィックを分析し、外部サイトをブラックリストに登録し、後で分析するためにユーザートラフィックをログに記録できるようにするには、次のソリューションのどれを実装する必要がありますか？
A. 侵入検知システム（IDS）

B. アプリケーションレベルのプロキシ
C. 回路レベルのプロキシ
D. ホストベースのファイアウォール
Answer: C (メーッセージを残す**)**

最新問題**: 204**
次のうち、通常、次の設計で考慮されないものはどれですか。
パスワード？
A. 生涯
B. 電子監視
C. 認証期間
D. 作曲
Answer: B (メーッセージを残す**)**
電子監視は、認証デバイスに送信されているパスワードを盗聴することです。この問題は技術的な問題であり、パスワードを設計する際の考慮事項ではありません。他の回答は、パスワードを開発するときに考慮しなければならない非常に重要なパスワードの特性に関連しています。パスワードの有効期間は、回答aで、パスワードが有効である最大期間を指します。理想的には、パスワードは1回だけ使用する必要があります。このアプローチは、トークンパスワードジェネレーターとチャレンジレスポンススキームによって実装できます。ただし、実際問題として、ほとんどのPCとワークステーションのパスワードは繰り返し使用されます。パスワードを変更する必要がある期間は、アクセスする情報に必要な保護レベルの関数です。典型的な組織では、パスワードは3〜6か月ごとに変更される場合があります。明らかに、従業員が組織を離れるとき、またはパスワードが危険にさらされている可能性がある状況では、パスワードを変更する必要があります。
回答 「パスワードの構成」は、パスワードに使用できる文字を定義します。文字は、文字、数字、または特殊記号の場合があります。
「認証期間」は、ユーザーの最初の認証からその後の再認証プロセスまでの最大許容期間を定義します。たとえば、重要な情報を含むサーバーにログオンしてから指定された期間が経過すると、ユーザーは再度認証を求められる場合があります。
トピック14、試験セットB

最新問題**: 205**
ジョブローテーション、責任の共有、監査記録のレビューなどの管理は、以下に関連しています。
A. 予防的/物理的。
B. 探偵/技術。
C. 探偵/物理。
D. 探偵/管理。
Answer: (解答を表示する**)**
説明/参照：
Explanation:
探偵の管理制御の例には、監視と監視、ジョブローテーション、および調査が含まれます。

不正解：
A：予防的物理的制御の例には、ロック、バッジシステム、警備員、生体認証システム、およびマントラップドアが含まれます。
B：探偵技術管理の例には、監査ログとIDSが含まれます。
C：探偵物理制御の例には、モーションディテクターや閉回路テレビが含まれます。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、2013、pp.28-34

最新問題: **206**
PPTPとL2TPの違いに関する次の記述の1つは正しくありません
A. PPTPはIPネットワーク上でのみ実行できます。
B. PPTPは暗号化プロトコルですが、L2TPは暗号化プロトコルではありません。
C. L2TPは、NATを実行するすべてのファイアウォールとネットワークデバイスで適切に機能します。
D. L2TPはAAAサーバーをサポートします
Answer: C (メーッセージを残す**)**
L2TPはパケットヘッダーの変更の影響を受け、ファイアウォールや
NATを実行するネットワークデバイス。
「PPTPはIPネットワーク上でのみ実行できます。」PPTPはデータグラムをIPにカプセル化するので正しいです
パケット。PPTPがIPネットワークを介して多くのネットワークプロトコルをルーティングできるようにします。
「PPTPは暗号化プロトコルですが、L2TPはそうではありません。」正しい。PPTPを使用する場合、PPPペイロード
MSCHAPまたはEAP-TLSを使用してMicrosoftPoint-to-PointEncryption（MPPE）で暗号化されます。
L2TPはTACACS+とRADIUS　をサポートしているため、「L2TPはAAAサーバーをサポートしています」は正しいです。
ノート：
L2TPはNATを介して機能します。すべてのパケットをにラップするトンネルモードを使用することが可能です。
UDPパケット。ポート4500はこの目的で使用されます。ただし、これはPPTPには当てはまらず、当てはまりません。
また、すべてのファイアウォールとNATデバイスでうまく機能します。
参照：
オールインワン第3版545ページ
CISSP試験の公式ガイドページ124-126

最新問題: **207**

ソフトウェア製品の開発段階で多層防御をサポートするために使用されるのは、次のうちどれですか？
A. 既知の脆弱性リスト
B. メンテナンス
C. ポリインスタンス化
D. セキュリティ監査
Answer: (解答を表示する**)**

最新問題**: 208**
情報システムの計画外のダウンタイムのほとんどは、次のうちどれに起因しますか？
A. ヒューマンエラー
B. 自然災害
C. ハードウェア障害
D. ソフトウェア障害
Answer: C (メーッセージを残す**)**

最新問題**: 209**
レガシーシングルサインオン $SO)は次のとおりです。
A. ユーザーが同じユーザーを入力することですべてのアプリケーションに対して認証できるようにするテクノロジー
毎回IDとパスワードを使用するため、覚えておく必要のあるパスワードは1つだけです。
B. 複数のプラットフォーム間で一貫してパスワードを管理し、パスワード変更間隔などのポリシーを適用するテクノロジー。
C. ユーザーが自分自身を一度認証してから、資格情報の中央リポジトリを使用してさまざまなレガシーアプリケーションを起動できるメカニズム。
D. SESAMEとKryptoKnightを参照する別の方法。現在、Kerberosは事実上の業界標準のシングルサインオンメカニズムです。
Answer: (解答を表示する**)**
ユーザーが自分自身を一度認証してから、資格情報の中央リポジトリを使用してさまざまなレガシーアプリケーションを起動できるメカニズム。
次の答えは正しくありません。
ユーザーが毎回同じユーザーIDとパスワードを入力することにより、すべてのアプリケーションに対して認証できるようにするテクノロジー。これにより、1つのパスワードのみを覚える必要があります。
これは中傷者です。ユーザーは各アクセス試行のユーザーIDとパスワードを入力しているため、これはSSOの説明でもないことに注意してください。
複数のプラットフォーム間で一貫してパスワードを管理し、パスワード変更間隔などのポリシーを適用するテクノロジー。
これは、ID管理パスワード管理システムについては適切な説明ですが、レガシーSSOについては適切な説明ではありません。

SESAMEとKryptoKnightを参照する別の方法として、Kerberosが事実上の業界標準のシングルサインオンメカニズムになっています。これは中傷者です。
この質問を作成するために、次の参照が使用されました。
CISSP CBK 2007の公式（ISC）2ガイド、176ページ：
多くのレガシーシステムは、ユーザーを識別および認証するための外部手段をサポートしていません。
したがって、さまざまなアプリケーションの外部にクレデンシャルを保存し、アプリケーションの起動時にユーザーに代わってクレデンシャルを自動的に入力することができます。」

最新問題: **210**
Kerberosに関する次の説明のうち正しいものはどれですか？
A. Kerberosは公開鍵暗号を使用します。
B. KerberosはX.509証明書を使用します。
C. Kerberosはクレデンシャルベースの認証システムです。
D. KerberosはMicrosoftによって開発されました。
Answer: C (メーッセージを残す**)**
Kerberosは、MITで開発された信頼できる資格ベースのサードパーティ認証プロトコルであり、対称（秘密キー暗号化を使用して、サービスにアクセスするためにネットワーク上の他のエンティティに対してクライアントを認証します。使用しません
X.509証明書。公開鍵暗号で使用されます。
出典：KRUTZ、Ronald L. & VINES、Russel D.、CISSP準備ガイド：マスタリング
コンピュータセキュリティの10のドメイン、John Wiley & Sons、2001年、第2章：アクセス制御システム（40ページ）。

最新問題: **211**
次のバックアップサイトのうち、災害復旧に最も効果的なのはどれですか？
A. タイムブローカー
B. ホットサイト
C. コールドサイト
D. 相互合意
Answer: B (メーッセージを残す**)**
説明/参照：
Explanation:
ホットサイトは、サイトをできるだけ早く利用できるようにする必要がある企業にとっては良い選択です。ホットサイトから欠落しているリソースは通常、データだけです。ホットサイトとは、リースまたはレンタルされ、完全に構成され、数時間以内に運用できるようになっている施設です。
不正解：

A :タイムブローカーのバックアップソリューションは、ホットサイトやコールドサイトに比べて効果が低くなります。
C :コールドサイトは、基本的な環境、電気配線、空調、配管、フローリングを提供する賃貸または賃貸施設であるため、ホットサイトよりも効果が低くなりますが、機器や追加サービスは提供されません。コールドサイトは本質的に空のデータセンターです。
D：相互合意は強制可能であるため、相互合意はホットサイトまたはコールドサイトと比較して効果が低くなります。つまり、A社はB社が必要に応じて施設を利用できると述べたが、必要が生じた場合、A社は法的にこの約束を果たす必要はないということである。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、2013、p。921

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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: **212**
リンク暗号化について正しいのは次のうちどれですか？
A. 各エンティティには、宛先ノードとの共通キーがあります。
B. 暗号化されたメッセージは、最終ノードによってのみ復号化されます。
C. このモードは、伝送パスに沿ったノードのいずれかが危険にさらされた場合の保護を提供しません。
D. このタイプの送信ではセキュアノードのみが使用されます。
Answer: (解答を表示する**)**
リンク暗号化では、各エンティティには、次の2つの隣接ノードと共通のキーがあります。
トランスミッションチェーン。
したがって、ノードは前のノードから暗号化されたメッセージを受信し、それを復号化してから、再送信します。
後続ノードに共通の新しいキーで暗号化します。明らかに、このモードは提供しません
伝送パスに沿ったノードのいずれかが危険にさらされた場合の保護。
暗号化は、それぞれ異なるタイプの異なる通信レベルで実行できます。
保護と影響。暗号化実装の2つの一般的なモードは、リンク暗号化です。
エンドツーエンド暗号化。
リンク暗号化は、衛星リンクT3のように、特定の通信パスに沿ってすべてのデータを暗号化します
回線、または電話回線。ユーザー情報が暗号化されるだけでなく、ヘッダー、トレーラー、

アドレス、およびパケットの一部であるルーティングデータも暗号化されます。唯一のトラフィックは
このテクノロジーで暗号化されているのは、データリンク制御メッセージング情報です。
さまざまなリンクデバイスが通信を同期するために使用する命令とパラメータ
メソッド。リンク暗号化は、パケットスニファおよび盗聴者に対する保護を提供します。
エンドツーエンド暗号化では、ヘッダー、アドレス、ルーティング、およびトレーラー情報は
暗号化されているため、攻撃者はキャプチャされたパケットとその送信先について詳しく知ることができます。
この質問に使用される参照：
ハリス、ション 2012-10-25）。CISSPオールインワン試験ガイド、第6版 pp.845-846）。マグロウヒル。
と：
KRUTZ、Ronald L.＆VINES、Russel D.、CISSP準備ガイド :の10のドメインをマスターする Computer Security、John Wiley＆Sons、2001年、第4章：暗号化182ページ）。

最新問題**: 213**
消火システムに関する次の説明のうち、正しいものはどれですか。
A. ハロンは、火の中の元素の化学反応を妨げるという点で非常に効果的であるため、エージェントに関する限り、今日最も一般的な選択肢です。
B. ガスマスクは、CO2システムの使用に対する効果的な保護を提供します。データセンター内の従業員を保護するために推奨されます。
C. CO2システムは、火災を維持するために必要な酸素供給を抑制するため、効果的ではありません。
D. 水ベースの消火器は、クラスC（電気）火災に効果的な消火方法ではありません。
Answer: D (メーッセージを残す**)**
説明/参照：
Explanation:
クラスCの火災は、電気機器または配線で発生する可能性のある電気火災です。クラスC消火器は、ガス、CO2、または乾燥粉末を使用します。これらの消火剤は非導電性です。
クラスA消火器は水または泡を使用します。電気火災に使用される水または泡は、電気を伝導し、火災を悪化させます。したがって、水ベースの消火器は、クラスC（電気）火災に効果的な消火方法ではないことは事実です。
不正解：
A :エージェントに関する限り、ハロンは最も一般的な選択肢ではありません。ハロンは現在危険であることが知られており、もはや生産されていません。したがって、この答えは正しくありません。
B :ガスマスクはCO2システムの使用に対する効果的な保護を提供しません。CO2システムは、空気から酸素を取り除くことによって機能します。したがって、この答えは正しくありません。
C :CO2システムは、火災を維持するために必要な酸素供給を抑制するため、効果的です。

したがって、この答えは正しくありません。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、2013、p。472

最新問題: **214**
知的財産権は、次のうちどれに主に関係していますか？
A. 配送方法を管理する所有者の権利
B. 金銭的利益を実現する所有者の能力
C. 所有者が自分たちの創造を楽しむ権利
D. 著作権を維持する所有者の能力
Answer: (解答を表示する**)**

最新問題: **215**
パッチが組織のシステムに適用される場合、パッチの互換性の効果的なテストを最もよくサポートするのは次のうちどれですか？
A. デバイスの標準化された構成
B. 標準化されたパッチテスト機器
C. 自動システムパッチ
D. パッチ適用の管理サポート
Answer: (解答を表示する**)**
説明
セクション :セキュリティの評価とテスト

最新問題: **216**
アウトソーシングされたソフトウェア開発で発生するセキュリティ上の欠陥を最もよく防ぐことができるのは、次のうちどれですか？
A. コード品質に関する契約上の要件
B. 行われた作業の品質と正確さの証明
C. ライセンス、コードの所有権、知的財産権
D. 納期、変更管理管理、予算管理
Answer: (解答を表示する**)**

最新問題: **217**
質問に答えるには、以下の情報を参照してください。
組織は、セキュリティ部門を率いるために情報セキュリティ責任者を雇っています。
役員には十分な人的資源がありますが、効果的なセキュリティプログラムを実施するために必要な他のコンポーネントが不足しています。セキュリティへの関与を必要とする多くのイニシアチブがあります。
セキュリティプログラムは、次の場合に効果的であると見なすことができます。
A. バックアップは定期的に実行され、検証されます。

B. 脆弱性は事前に特定されます。
C. 監査は定期的に実施され、レビューされます。
D. リスクは許容レベルまで低下します。
Answer: D (メーッセージを残す**)**

最新問題**: 218**
リレーショナルデータベースでは、次の方法でデータにアクセスするためのセキュリティが提供されます。
A. 候補キー。
B. ビュー。
C. 参加します。
D. 属性。
Answer: B (メーッセージを残す**)**
正解はビューです。候補キーは、のセットです
主キーが選択される一意のキー。回答が参加します
データベースで実行できる操作を示し、
属性は、リレーショナルテーブルの列を示します。

最新問題**: 219**
契約や契約は、多くの場合、執行不能または執行が困難です。次の代替施設復旧契約のどれですか？
A. ホットサイト。
B. 暖かい場所。
C. コールドサイト。
D. 相互合意。
Answer: D (メーッセージを残す**)**
説明/参照：
Explanation:
相互合意は強制力があります。つまり、A社はB社が必要に応じて施設を利用できると述べたが、必要が生じた場合、A社は法的にこの約束を果たす必要はないということである。
不正解：
A :ホットサイト契約は強制力がありますが、相互契約は強制力がない場合があります。
B :ウォームサイト契約は強制力がありますが、相互合意は実行するのが難しい場合があります。
C :コールドサイト契約は強制力がありますが、相互合意は実行するのが難しい場合があります。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、2013、p。924

最新問題**: 220**
次のうち、モバイルコードの例はどれですか？
A. 制御システムに埋め込まれたコード

B. スパイラルモデルに従って導出されたコード
C. PCに埋め込まれたコード
D. からWebブラウザにダウンロードされたJavaおよびActiveXコード
ワールドワイドウェブ（WWW）
Answer: D (メーッセージを残す**)**
モバイルコードの例はJavaと
WorldWideからWebブラウザにダウンロードされたActiveXコード
ウェブ。他の答えはコードの種類であるため正しくありません
モバイルコードとは関係ありません。

最新問題**: 221**
伝送制御プロトコル/インターネットプロトコル（TCP / IP）スタックで、別のノードとの接続のネゴシエーションと確立を担当するレイヤーはどれですか？
A. トランスポート層
B. アプリケーション層
C. セッション層
D. ネットワーク層
Answer: A (メーッセージを残す**)**

最新問題**: 222**
次のプラクティスのうち、ソフトウェアの設計におけるセキュリティの定義と脅威の特定を開発チームに提供するのはどれですか？
A. 要件レビュー
B. 脅威モデリング
C. 侵入テスト
D. 利害関係者のレビュー
Answer: (解答を表示する**)**

最新問題**: 223**
隠密チャネルを最もよく定義するものは何ですか？
A. オペレーティングシステムにプログラマーが残した文書化されていないバックドア
B. 閉じる必要がある開いているシステムポート。
C. システムのセキュリティポリシーに違反する方法で情報を転送できるようにする通信チャネル。
D. トロイの木馬。
Answer: (解答を表示する**)**
秘密チャネルは、エンティティが不正な方法で情報を受信するための方法です。これは、セキュリティメカニズムによって制御されない情報フローです。このタイプの情報パスは、通信用に開発されたものではありません。したがって、開発者は情報がこのように渡されることを想定していなかったため、システムはこのパスを適切に保護しません。

この方法で情報を受信すると、明らかにシステムのセキュリティポリシーに違反します。この無許可のデータを転送するチャネルは、次のいずれかの条件の結果です。*
製品開発の監督
*アクセス制御の不適切な実装
*2つのエンティティ間の共有リソースの存在
*トロイの木馬のインストール
次の答えは正しくありません。
プログラマーがオペレーティングシステムに残した文書化されていないバックドアは、情報の不正な転送が行われる手段ではないため、正しくありません。このようなバックドアは通常、メンテナンスフックと呼ばれます。
閉じるべき開いているシステムポートは、隠れチャネルを定義していないため、正しくありません。
トロイの木馬は便利なプログラムのように見えるため正しくありませんが、インストールすると、インストーラーが知らないうちにワーム、バックドア、その他のマルウェアなどのボーナスが含まれます。
この質問に使用される参照：
ションハリスAIOv3、第5章 :セキュリティモデルとアーキテクチャ
AIOv4セキュリティアーキテクチャと設計（343～344ページ）
AIOv5セキュリティアーキテクチャと設計（345～346ページ）

最新問題: **224**
一定の時間間隔で一意のパスワードを生成するトークンは、次のように呼ばれます。
A. 同期動的パスワードトークン。
B. チャレンジ/レスポントークン。
C. 時間に敏感なトークン。
D. 非同期の動的パスワードトークン。
Answer: A (メーッセージを残す**)**
正解は「同期動的パスワードトークン」です。

最新問題: **225**
次のうち、Webベースのクライアント側の入力検証の使用に関連する脅威はどれですか？
A. Webサーバーは送信後に入力を検証できません
B. 検証が行われた後、ユーザーは入力を変更できます
C. Webサーバーはクライアントから無効な入力を受け取ることができません
D. クライアントシステムがWebサーバーから無効な入力を受け取る可能性があります
Answer: B (メーッセージを残す**)**

最新問題: **226**
次のファイアウォールルールのうち、組織の内部ネットワークとインターネットの間にインストールされているファイアウォールで見つかる可能性が低いのはどれですか？

A. ローカルホストとの間のすべてのトラフィックを許可します。
B. すべてのインバウンドsshトラフィックを許可する
C. すべてのインバウンドTCP接続を許可します。
D. log-server.abc.orgへのすべてのsyslogトラフィックを許可します。
Answer: C (メーッセージを残す**)**
オプション C」は、そのインターフェースの1つをインターネットなどのパブリックネットワークに接続するファイアウォールでは非常に悪い習慣です。このルールでは、すべてのインバウンドTCPトラフィックを許可しているため、ハッカーは必要なすべての攻撃を任意のTCPポートに送信でき、ポートスキャン、Syn攻撃、およびその他の多くの危険なDoSアクティビティをプライベートネットワークに送信できます。
ローカルホストからのトラフィックを許可することがベストプラクティスであり、ファイアウォールがローカルホストです。SSHを許可する
セキュアシェル）このプロトコルは暗号化を使用するため、これも優れています。

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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**: 227**
次の運用セキュリティ制御のうち、許可されていない侵入者がシステムに内部または外部からアクセスするのを防ぎ、システムに侵入する意図しないエラーの量と影響を減らすことを目的としているのはどれですか？
A. 探偵コントロール
B. 予防管理
C. 修正コントロール
D. ディレクティブコントロール
Answer: B (メーッセージを残す**)**
説明/参照：
Explanation:
予防管理。運用セキュリティドメインでは、予防制御は、システムに侵入する意図しないエラーの量と影響を減らすことと、許可されていない侵入者がシステムに内部または外部からアクセスすることを防ぐことの2つのことを実現するように設計されています。これらのコントロールの例としては、事前に番号が付けられたフォームや、重複を防ぐためのデータ検証およびレビュー手順があります。
不正解：

A：検出コントロールは、エラーが発生したときにエラーを検出するために使用されます。許可されていない侵入者がシステムの内部または外部にアクセスするのを防ぐことはできません。
C：データ回復手順を通じて損失イベントの影響を軽減するのに役立つ修正制御が実装されています。許可されていない侵入者がシステムの内部または外部にアクセスするのを防ぐことはできません。
D：指令管理は、ポリシー、手順、ガイドライン、合意などの管理手段です。許可されていない侵入者がシステムの内部または外部にアクセスするのを防ぐことはできません。
参照：
Krutz、Ronald L. and Russell Dean Vines、CISSP Prep Guide：Mastering the CISSP and ISSEP Exams、2nd Edition、Wiley Publishing、Indianapolis、2004、p。217。

最新問題: **228**
侵入や攻撃による被害を防ぐために最も適切な対策は次のうちどれですか？
A. そのような活動の監視と監査
B. ユーザー認証が必要
C. 必要な電話番号のみが公開されていることを確認する
D. 音声アクセスとデータアクセスにまったく異なる番号を使用する
Answer: B (メーッセージを残す**)**
攻撃者は範囲内のすべての番号をダイヤルすることでモデム番号を発見できるため、モデム番号の知識は不十分なアクセス制御方法です。リモートアクセスが許可される前にユーザー認証を要求すると、モデム回線を介した不正アクセスを回避するのに役立ちます。
「そのような活動の監視と監査」は正しくありません。監視と監査は、ウォーディアル攻撃の検出に役立ちますが、ウォーディアル攻撃の成功を防ぐことはできません。
「必要な電話番号だけを公開する」というのは誤りです。ウォーディアリング攻撃は範囲内のすべての番号を盲目的に呼び出すため、範囲内の特定の番号が公開されているかどうかは関係ありません。
「音声アクセスとデータアクセスにまったく異なる番号を使用する」は正しくありません。音声アクセスとデータアクセスに異なる番号範囲を使用すると、攻撃者がパブリック音声番号範囲を監視しているときにデータラインに遭遇するのを防ぐのに役立つ場合がありますが、これは適切な対策ではありません。
参照：
CBK、p。214
AIO3、p。534-535

最新問題: **229**
バイオメトリクスは、物理的制御における識別および
での認証：
A. 探偵コントロール。
B. 修正コントロール。

C. 論理制御。
D. 予防管理。
Answer: (解答を表示する**)**
正解は「論理制御」です。他の回答は、攻撃が発生する前に予防的コントロールが脆弱性を排除または削減しようとする、さまざまなカテゴリのコントロールです。探偵コントロールは、攻撃が行われている、または行われたことを判断しようとします。修正制御には、攻撃が成功した後、システムを通常の動作に戻すためのアクションを実行することが含まれます。

最新問題: **230**
国防総省のマルチレベルの軍事安全保障政策を抽象的な正式な言葉で最初に説明したのは誰ですか？
A. デビッド・ベルとレナード・ラパドゥラ
B. リベスト、シャミール、エーデルマン
C. ホイットフィールドディフィーとマーティンヘルマン
D. デビッド・クラークとデビッド・ウィルソン
Answer: A (メーッセージを残す**)**
1973年に最初に説明したのはデビッドベルとレナードラパドゥラでした
抽象的で正式な用語でのDoDマルチレベル軍事セキュリティポリシー。ベルラパドゥラは
機密性に関係する強制アクセス制御（MAC）モデル。リベスト、シャミール、
Adleman（RSA）は、RSA暗号化アルゴリズムを開発しました。ホイットフィールド・ディフィーとマーティン
ヘルマンは1976年にDiffie-Hellman鍵合意アルゴリズムを公開しました。DavidClarkと
David Wilsonは、商業活動のセキュリティにより適したClark-Wilson整合性モデルを開発しました。
出典：RUSSEL、Deborah＆GANGEMI、GT Sr.、Computer Security Basics、O'Reilly、
1992年7月（78,109ページ）。

最新問題: **231**
適切に分離された環境で互換性のある機能は次のうちどれですか？
A. システムプログラミングとジョブ制御分析
B. アプリケーションプログラミングとコンピューター操作
C. アクセス許可とデータベース管理
D. システム開発とシステムメンテナンス
Answer: (解答を表示する**)**

最新問題: **232**
次のうち、インターネットプロトコルセキュリティ（IPSec）のキー交換を定義するものはどれですか？
A. セキュリティキー交換（SKE）
B. インターネット制御メッセージプロトコル（ICMP）

C. インターネットキーエクスチェンジ（IKE）
D. Secure Sockets Layer（SSL）キー交換
Answer: C (メーッセージを残す)

最新問題**: 233**
Object Request Broker（ORB）を使用して実装する標準
異種の分散環境でのオブジェクト間の交換
と呼ばれます：
A. インターフェース定義言語（IDL）
B. オープンアーキテクチャ
C. Object Management Group（OMG）オブジェクトモデル
D. Common Object Request Broker Architecture（CORBA）
Answer: D (メーッセージを残す)
* OMGオブジェクトモデルは、オブジェクトの外部から見える特性を記述するための標準的な手段を提供します。
* AnswerOpenArchitectureは気を散らすものです。
* IDLは、標準のインターフェース言語です。
クライアントがオブジェクトからサービスを要求するために使用します。

最新問題**: 234**
安全な状態の概念、アクセスのモード、およびアクセスを許可するためのルールを定義するために使用されるマルチレベルセキュリティポリシーの最初の数学モデルの名前は何ですか？
A. クラークとウィルソンのモデル
B. ハリソンルッゾウルマンモデル
C. リベストとシャミールモデル
D. ベルラパドゥラモデル
Answer: D (メーッセージを残す)
出典：TIPTON、Hal、（ISC）2、CISSP試験プレゼンテーションの概要。

最新問題**: 235**
通常、どのサービスがポート25で実行されますか？
A. ファイル転送プロトコル（FTP）
B. Telnet
C. SMTP（Simple Mail Transfer Protocol）
D. ドメインネームサービス（DNS）
Answer: C (メーッセージを残す)
説明/参照：
Explanation:
SMTPはポート25を使用します。
不正解：

A :FTPはポート21を使用します。
B :Telnetはポート23を使用します。
D :DNSはポート53を使用します。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、New York、2013、p。1289

最新問題: **236**
Kerberosに関する次の説明のうち正しいものはどれですか？
A. Kerberosは公開鍵暗号を使用します。
B. KerberosはX.509証明書を使用します。
C. Kerberosはクレデンシャルベースの認証システムです。
D. KerberosはMicrosoftによって開発されました。
Answer: (解答を表示する**)**
Kerberosは、MITで開発された信頼できる資格ベースのサードパーティ認証プロトコルであり、対称（秘密キー暗号化を使用して、サービスにアクセスするためにネットワーク上の他のエンティティに対してクライアントを認証します。公開鍵暗号化で使用されるX.509証明書は使用しません。
出典 :KRUTZ、Ronald L.＆VINES、Russel D.、CISSP Prep Guide :Mastering the Ten Domains of Computer Security、John Wiley＆Sons、2001年、第2章 :アクセス制御システム 40ページ）。

最新問題: **237**
以下の質問のうち、リスクのプロセスに関して正確ではないものはどれですか
評価？
A. リスク評価はリスク管理の最終結果です
方法論。
B. 脅威の可能性は、
リスクアセスメント。
C. リスク評価は、リスク管理の最初のプロセスです
方法論
D. 脅威の影響のレベルは、次の要素として決定する必要があります。
リスク評価。
Answer: A (メーッセージを残す**)**
リスクは、特定の脅威ソースが特定の潜在的な脆弱性を行使する可能性と、その結果として生じる組織への有害事象の影響の関数です。リスク評価は、リスク管理方法論の最初のプロセスです。
リスク評価
プロセスは、組織が削減のための適切なコントロールを特定するのに役立ちます
またはリスク軽減プロセス中にリスクを排除します。
将来の有害事象の可能性を判断するために、
ITシステムは、潜在的な脆弱性およびITシステムに導入されている制御と併せて分析する必要があります。特定の脅威ソースによって潜在的な脆弱性が行使される可能性は、高、中、または低と

して説明できます。影響とは、脅威による脆弱性の悪用によって引き起こされる可能性のある危害の大きさを指します。影響のレベルを決定すると、
影響を受けるIT資産とリソースの相対的な価値。出典 :NIST
特別刊行物800-30、情報技術システムのリスク管理ガイド。

最新問題: **238**
パケット交換技術ではないのはどれですか？
A. フレームリレー
B. SMDS
C. X.25
D. T1
Answer: (解答を表示する**)**
正解はT1です。T1回線は、専用のポイントツーポイントテクノロジを使用する専用回線の一種です。

最新問題: **239**
データベースの暗号化に最適なDES操作モードはどれですか？
A. 暗号ブロック連鎖（CBC）モード
B. 巡回冗長検査（CRC）モード
C. 電子コードブック（ECB）モード
D. 暗号フィードバック（CFB）モード
Answer: (解答を表示する**)**
電子コードブック（ECB）モードのDESアルゴリズムは、対称鍵管理が採用されている場合、DEKおよびMIC暗号化に使用されます。カプセル化されたPEMヘッダーフィールド内の文字列「DES-ECB」は、このアルゴリズム/モードの組み合わせの使用を示します。
対称鍵管理をサポートする準拠PEM実装は、このアルゴリズム/モードの組み合わせをサポートする必要があります。このDES暗号化モードは、オーバーヘッドが低いため、データベース暗号化に最適です。
ECBモードにはいくつかの弱点があります。ここにそれらがあります：
1。ECBモードは、他のすべての64ビットブロックとは独立して64ビットブロックを暗号化します
2。同じキーが与えられると、同一の平文は同じ方法で暗号化されます
3。ECBの前のデータ圧縮が役立ちます（他のモードと同様）
4。ブロックサイズは64ビットに固定されているため、不完全なブロックはパディングする必要があります

最新問題: **240**
NISTが新しいAdvancedEncryptionStandard用に選択した暗号化アルゴリズムを特定するのは次のうちどれですか？
A. Twofish
B. 蛇

C. RC6
D. Rijndael
Answer: D (メーッセージを残す)
説明/参照：
Explanation:
DESが20年以上暗号化標準として使用され、必要な技術が利用可能になると比較的短時間で解読された後、NISTは新しい標準であるAdvanced Encryption Standard（AES）を導入する必要があると判断しました。1997年1月、NISTはAES候補の要求を発表し、FIPS PUB 197の要件の概要を説明しました。AESは、128、192、および256ビットのキーサイズをサポートする対称ブロック暗号である必要がありました。次の5つのアルゴリズムがファイナリストでした。
ルシファーを作成したIBMチームによって開発されたMARS
- RSAラボラトリーズによって開発されたRC6
- ロス・アンダーソン、エリ・ビアム、ラース・クヌードセンによって開発された蛇
- CounterpaneSystemsによって開発されたTwofish
- RijndaelJoanDaemenとVincentRijmenによって開発されました
- これらの出場者の中から、Rijndaelが選ばれました。Rijndaelがサポートするブロックサイズは128、192、および
256ビット。
Rijndaelは、さまざまな製品や環境のソフトウェアやハードウェアに実装するとうまく機能します。メモリ要件が低く、タイミング攻撃から簡単に防御できるように構築されています。
Rijndaelは、DESに代わるNISTの選択でした。これは現在、機密であるが分類されていない米国政府の情報を保護するために必要なアルゴリズムです。
不正解：
A：Twofishはファイナリストでした。ただし、Rijndaelは、新しいAdvancedEncryptionStandardのNISTによって選択されました。
B：サーペントはファイナリストでした。ただし、Rijndaelは、新しいAdvancedEncryptionStandardのNISTによって選択されました。
C：RC6はファイナリストでした。ただし、Rijndaelは、新しいAdvancedEncryptionStandardのNISTによって選択されました。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、2013、p。809

最新問題: **241**
カスタムアプリケーションコードをテストする最も効果的な方法は何ですか？
A. 侵入テスト
B. ネガティブテスト
C. ブラックボックステスト
D. ホワイトボックステスト

Answer: D (メーッセージを残す)

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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: **242**
通常の電圧を下回る長時間の電源装置は次のとおりです。
A. サージ
B. 障害
C. 電圧低下
D. 停電
Answer: (解答を表示する)

最新問題: **243**
ユーザーIDを検証するためにどのような種類の証明書が使用されますか？
A. 公開鍵証明書
B. 属性証明書
C. ルート証明書
D. コード署名証明書
Answer: A (メーッセージを残す)
暗号化では、公開鍵証明書（またはID証明書）は、デジタル署名を組み込んだ電子文書であり、公開鍵とID（個人または組織の名前、住所などの情報）を結び付けます。証明書を使用して、公開鍵が個人に属していることを確認できます。
一般的な公開鍵インフラストラクチャ（PKI）スキームでは、署名は認証局（CA）のものになります。Web of Trustスキームでは、署名はユーザー（自己署名証明書または他のユーザー（承認））のいずれかです。いずれの場合も、証明書の署名は、ID情報と公開鍵が一緒に属していることを示す証明書署名者による証明です。
コンピュータセキュリティでは、認証証明書（属性証明書とも呼ばれます）は、発行者が制御する、または使用するためのアクセス権を持つサービスまたはリソースを使用するための発行者からの書面による許可を説明するデジタルドキュメントです。権限を委任することができます。
PKCとACを常に混同している人もいます。類推によって区別が明確になる場合があります。PKCはパスポートのようなものと見なすことができます。PKCは所有者を識別し、長期間使用する傾向があり、簡単に入手することはできません。ACは入国ビザのようなものです。通常、ACは別の機関によって発行され、長期間は持続しません。入国ビザを取得するには通常パスポートを提示する必要があるため、ビザの取得はより簡単なプロセスになる可能性があります。

この実際の例は、大規模なサービスプロバイダーによるモバイルソフトウェアの展開に見られ、通常、Microsoftスマートフォン および関連）、Symbian OS、J2MEなどのプラットフォームに適用されます。
これらの各システムでは、モバイル通信サービスプロバイダーは、モバイル端末クライアントの配布 つまり、携帯電話のオペレーティングシステムまたはアプリケーション環境）をカスタマイズして、「ファームウェアの更新」などの一連の機能またはアクセス許可にそれぞれ関連付けられた1つ以上のルート証明書を含めることができます。「 名簿へのアクセス」、 無線インターフェースの使用」、そして最も基本的なもの、「インストールして実行」。開発者がこれらの制御された環境の1つで配布と実行を有効にする場合は、適切なCA（通常は大規模な商用CA）から証明書を取得する必要があります。その過程で、通常、次のような帯域外メカニズムを使用してIDを検証します。電話、政府および商業データベースを介した法人の検証などの組み合わせ、
IDが検証されると、ソフトウェアへの署名に使用できるID証明書が発行されます。通常、開発者または発行者のID証明書によって署名されたソフトウェアは配布されませんが、特定のソフトウェアリリースに固有の認証証明書を生成する前に、コンテンツをテストまたはプロファイリングするためにプロセッサに送信されます。次に、その証明書は、配布の準備の最後のステップとしてソフトウェアに署名するために、一時的な非対称キーペアとともに使用されます。ID証明書と認証証明書を分離することには、特にシステムに受け入れられる新しいコンテンツのリスク軽減とキー管理、および攻撃ベクトルとして使用される可能性のある誤ったソフトウェアからの回復に関連する多くの利点があります。
参考資料 :HARRIS、ション、オールインワンCISSP認定試験ガイド、2001年、McGraw-Hill / Osborne、ページ
540. http://en.wikipedia.org/wiki/Attribute_certificate
http://en.wikipedia.org/wiki/Public_key_certificate

最新問題**: 244**
PKIインフラストラクチャのどこに、取り消された証明書のリストが保存されていますか？
A. CRL
B. 登録局
C. 回復エージェント
D. キーエスクロー
Answer: A (メーッセージを残す**)**
説明/参照：
Explanation:
公開鍵インフラストラクチャ PKI）では、証明書の失効は認証局 CA）によって処理されます。取り消された証明書情報は、証明書失効リスト CRL）に保存されます。
不正解：
B：登録局RA）が認証登録タスクを実行します。ただし、取り消された証明書のリストは保存されません。

C :キー回復エージェントは、デジタル証明書の意図された目的の1つです。ただし、取り消された証明書のリストは保存されません。
D :キーエスクローは、紛失または破損した暗号化キーを回復できるプロセスまたはエンティティです。ただし、取り消された証明書のリストは保存されません。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、2013、pp。833-836、843
Miller、David R、Microsoft CISSP Training Kit、O'Reilly Media、2013、California、p。217

最新問題**: 245**
* スター）整合性公理は、Bibaモデルではどういう意味ですか？
A. 読み上げなし
B. 書き留めなし
C. 読み上げなし
D. 書き込みなし
Answer: D (メーッセージを残す**)**
説明/参照：
Explanation:
Bibaモデルは、Bell-LaPadulaモデルの後に開発されました。ベルラパドゥラモデルに似たステートマシンモデルです。Bibaは、アプリケーション内のデータの整合性に対応しています。
Bibaモデルは、整合性レベルのラティスを使用します。適切に実装および実施された場合、Bibaモデルは、整合性レベルのデータがより高い整合性レベルに流れるのを防ぎます。
Bibaには、このタイプの保護を提供するための3つの主要なルールがあります。
*-整合性の公理 :サブジェクトは、より高い整合性レベルでオブジェクトにデータを書き込むことができません（「
書き上げる"）。
単純な整合性の公理 :サブジェクトは、より低い整合性レベルからデータを読み取ることができません（読み取りなし」と呼ばれます
下"）。
呼び出しプロパティ :サブジェクトは、より高い整合性のサービスを要求（呼び出す）できません。
不正解：
A :* スター）整合性の公理は、 読み取りなし」ではなく、 書き込みなし」を意味します。
B :* スター）整合性の公理は、 書き込みなし」ではなく 書き込みなし」を意味します。
C :* スター）整合性の公理は、 読み取りなし」ではなく、 書き込みなし」を意味します。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、New York、2013、p。372

最新問題**: 246**
保護する必要のある環境には、すべての人員、機器、データ、通信デバイス、電源、および配線が含まれます。必要な保護レベルは、データの価値、コンピューターシステム、および施設内の企業資

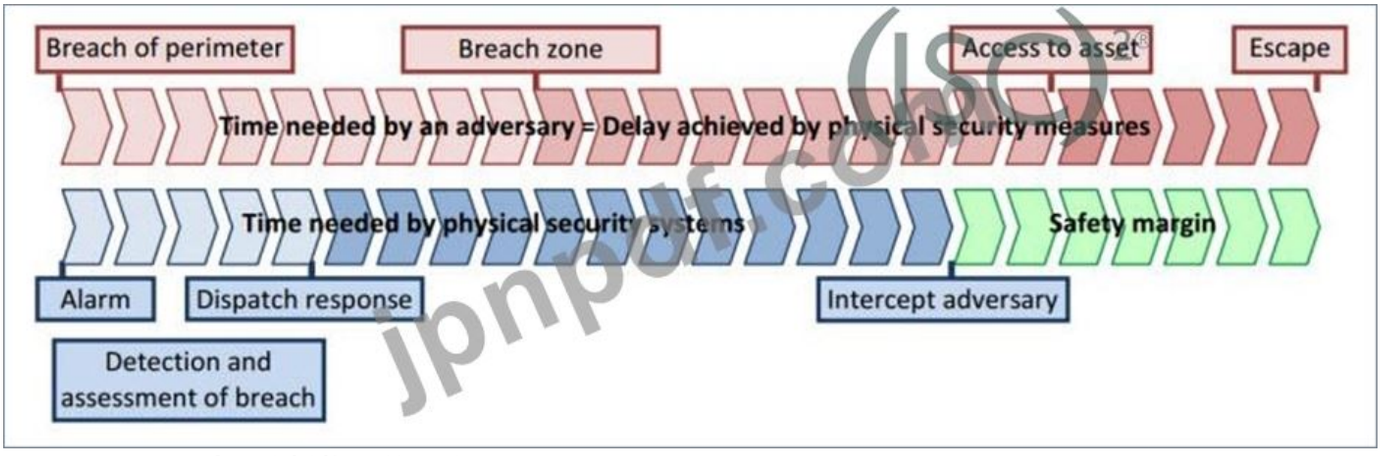
産によって異なります。これらの項目の価値は、どのような種類の分析によって決定できますか？

A. クリティカルチャネル分析
B. 被覆通信路分析
C. クリティカルパス分析
D. クリティカルコンジット分析

Answer: (解答を表示する**)**

セキュリティ制御の有効性は、対応チームが敵を妨害するのに十分な時間がある時点での検出の確率によって測定されます。クリティカルパスは、中断の可能性が最も低い敵のパスです。

敵対者の経路とは、資産が危険にさらされる可能性のある、資産に対する一連の順序付けられたアクションです。敵は通常、最も簡単で最も直接的なルートを取ることが期待できます。不正アクセスを早期に検出することで、より迅速な対応が可能になります。理想的には、資産にアクセスする前に傍受が発生する必要がありますが、これは資産とセキュリティの目的によって異なります。不正開封防止の証拠が資産を保護する目的である場合、中断は必要ない場合があります。以下の例を参照してください。



クリティカルパス分析物理的セキュリティ

CISSP試験と物理的セキュリティ

情報セキュリティは、コンピュータシステムが動作する物理的空間のセキュリティと管理に依存しています。CISSP試験の共通知識体系は、管理、技術、および物理的な制御を使用して、物理的なスペース、そのシステム、およびその中で働く人々を保護するという課題に対処します。

次のトピックについて説明します。

施設管理 :サイトの選択から緊急時の対応まで、物理的な運用スペースの保守と保護を管理する管理プロセス。

リスク、問題、および保護戦略 :リスクの特定とセキュリティ保護コンポーネントの選択。

境界セキュリティ：一般的な物理的保護制御。

要員派遣

施設管理は、安全な物理サイトの計画から物理情報システム環境の管理に至るまで、企業のセキュリティの複雑なコンポーネントです。施設管理の責任には、サイトの選択と物理的セキュリティ計画（つまり、施設の建設、設計とレイアウト、火災と水害の保護、盗難防止メカニズム、侵入

検知とセキュリティ手順）が含まれます。保護は人と資産の両方に及ぶ必要があります。必要な保護レベルは、資産とデータの価値によって異なります。
試験の候補者として、運用と交換のコストに関連するコンポーネントのビジネス機能の重要度を判断する手段として、クリティカルパス分析の概念を学ぶ必要があります。さらに、学生は安全な施設の最適な場所と物理的属性を理解する必要があります。このドメインでカバーされるトピックの中には、サイトの検査、場所、アクセス可能性と不明瞭さ、地域の犯罪率、および洪水や地震などの自然災害の可能性を考慮したものがあります。
試験のヒント：
このトピックは、物理的セキュリティの観点または論理的セキュリティのいずれかからのものである可能性があります
視点。
論理的な観点からは、次のように定義されます。ミッションクリティカルなアプリケーション間の関係を定義する分析。このタイプの分析は、ビジネスを継続するために何が起こらなければならないかを示すために実行されます。
この質問に使用される参照：
HARRIS、ション、オールインワンCISSP認定試験ガイド、McGraw-Hill / Osborne、2001、ページ281。
と
http://www.protectivesecurity.gov.au/physicalsecurity/Documents/Security-zones-and-risk-mitigation-control-measures.pdfおよび
http://www.onlineexpert.com/elearning/user/SampleFiles/SECURITY/CISSP_PS_Glossary。html

最新問題: **247**
次のうち、盗聴者からパスワードを保護し、通信の暗号化をサポートしているのはどれですか？
A. チャレンジハンドシェイク認証プロトコル（CHAP）
B. チャレンジハンドシェイク識別プロトコル（CHIP）
C. チャレンジハンドシェイク暗号化プロトコル（CHEP）
D. チャレンジハンドシェイク置換プロトコル（CHSP）
Answer: A (メーッセージを残す**)**
CHAP :3ウェイhanbdshakeを使用するプロトコルサーバーは、リプレイ攻撃を阻止するためにランダムな値（ナンス）を含むチャレンジをクライアントに送信します。クライアントは、ナンスのMD5ハッシュとパスワードで応答します。
クライアントの応答がサーバーが期待したものである場合、認証は成功します。
参照 :ページ450、OIG 2007
CHAPは、盗聴者からパスワードを保護し、通信の暗号化をサポートします。
参照 :KRUTZ、Ronald L.＆VINES、Russel D.、CISSP準備ガイド :マスタリング
コンピュータセキュリティの10のドメイン、2001年、John Wiley＆Sons、44ページ

最新問題: **248**

同値類のテストに関して正しいのは次のうちどれですか？
A. パーティション全体は、そのパーティションの代表的な値を1つだけ考慮することでカバーできます。
B. 関数に実装されたプロセスのステートレスな動作が特徴です。
C. テスト入力は、指定された機能仕様の派生境界から取得されます。
D. 通信プロトコルとグラフィカルユーザーインターフェイスのテストに役立ちます。
Answer: (解答を表示する**)**

最新問題**: 249**
アクセスドアに必要な基本的な電子アクセス制御（EAC）コンポーネントは、電磁ロックです。
A. クレデンシャルリーダーとドア閉センサー。
B. カードリーダーとドアオープンセンサー。
C. 生体認証リーダーとドアオープンセンサー。
D. カードリーダーとドアモーションディテクター。
Answer: A (メーッセージを残す**)**
この質問への参照を実際に見つけることができませんでした。そこで、「クレデンシャルリーダーとドア閉センサー」を使用します。
「スマートカードとダムカードに加えて、近接リーダーを使用して物理的なアクセスを制御できます。近接リーダーは、パッシブデバイス、フィールド電源デバイス、またはトランスポンダにすることができます。」--Ed Tittle CISSP学習ガイド（Sybex）pg 650

最新問題**: 250**
ホワイトボックステストとブラックボックステストの違いを最もよく表しているのは次のうちどれですか？
A. ホワイトボックステストは、独立したプログラマーチームによって実行されます。
B. ブラックボックステストはボトムアップアプローチを使用します。
C. ホワイトボックステストは、プログラムの内部論理構造を調べます。
D. ブラックボックステストにはビジネスユニットが関与します
Answer: (解答を表示する**)**
ブラックボックステストはシステムの外部動作を監視し、ホワイトボックステストは論理パスの詳細な検査であり、考えられる条件をチェックします。
出典：情報システム監査管理協会、認定情報システム
Auditor 2002レビューマニュアル、第6章 :ビジネスアプリケーションシステム開発、
取得、実装、および保守（299ページ）。

最新問題**: 251**
大規模な組織でシステムの重要度の分類が重要なのはなぜですか？
A. 所有権の決定が容易になり、資産のステータスに関する混乱が減ります。
B. 重要なシステムサポートの作業負荷を軽減し、パッチの適用に必要な時間を短縮します。

C. 経営幹部への明確なシステムステータスコミュニケーションを可能にします。
D. セキュリティおよびメンテナンスタスクの適切な優先順位付けとスケジューリングを提供します。
Answer: (解答を表示する**)**

最新問題**: 252**
認証プロセスの主な結果は、文書化されたものを提供することです
A. 相互接続されたシステムとそれらに実装されたセキュリティ制御。
B. セキュリティ評価、テスト、およびプロセス評価の基準。
C. 修復のためのシステムの弱点。
D. リスクベースの意思決定を行うために必要なセキュリティ分析。
Answer: D (メーッセージを残す**)**
セクション :ソフトウェア開発のセキュリティ

最新問題**: 253**
階層ストレージ管理（HSM）は、一般的に次の場所で使用されます。
A. 非常に大規模なデータ検索システム。
B. 非常に小さなデータ検索システム。
C. より短いデータ検索システム。
D. ほとんどのデータ検索システム。
Answer: A (メーッセージを残す**)**
説明/参照：
Explanation:
HSM（Hierarchical Storage Management）は、継続的なオンラインバックアップ機能を提供します。ハードディスクテクノロジーと、安価で低速なオプティカルジュークボックスまたはテープジュークボックスを組み合わせています。HSMは通常、非常に大規模なデータ検索システムで使用されます。
不正解：
B :HSMは通常、小規模なデータ検索システムでは使用されません。
C :HSMは小さなデータ検索システムでは使用されません。
D :HSMはさらに複雑になるため、非常に大規模なデータ検索システムでのみ使用されます。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、New York、2013、p。1274

最新問題**: 254**
あなたの財産保険に実際の現金評価（ACV）条項がある場合、あなたの損害を受けた財産は以下に基づいて補償されます：
A. 紛失日の商品の価値
B. 紛失したアイテムの状態に関係なく、古いアイテムを新しいアイテムに交換する
C. 損失の1か月前のアイテムの価値

D. 損失日のアイテムの価値に10%を加えたもの
Answer: A (メーッセージを残す**)**
これは、実際の現金価値 ACV）または実際のコスト評価 ACV）と呼ばれます。
他のすべての答えはただの批判者でした。以下に、さまざまなタイプの説明があります
あなたが使用できる評価の。保険会社にどちらを検証するかを確認することは非常に重要です。
あなたが災害を起こした日を見つけるのに非常に驚くべきことがあるかもしれないのであなたに当てはまります
起こる。
交換費用
不動産交換費用保険は、古いものを新しいものに交換することを約束します。一般的に、
建物は同じ敷地内で同じ目的で使用され、材料を使用する必要があります
損傷または破壊された資産の材料の品質に匹敵します。
この約束には他にもいくつかの制限があります。たとえば、修理や交換の費用
建物用
建築基準法やその他の方法を管理する法律に関連するコストの増加は含まれていません
建物は今日建てられなければなりません。建物の運営のための補償範囲を追加する承認
コードとそれらの遵守に関連するコストの増加は、個別に入手できます-
通常、追加のプレミアムが必要です。
さらに、一部の保険引受会社は、減価償却額で特定の資産のみをカバーします
（実際の現金価値-ACV）建物に取り付けられている場合でも基準。これには日よけと
床の敷物、冷蔵、換気、調理、食器洗い、および洗濯用の器具。
減価償却額は、屋外設備または家具にも適用されます。
実際の現金価値 ACV）
ACVは、商業用不動産保険のデフォルトの評価条項です。別名
減価償却額ですが、これは会計上の減価償却額と同じではありません。実際の現金価値は、最初に物件の交換価値を計算することによって決定されます。次のステップでは、建物の築年数、摩耗、破損を反映して、差し引く金額を見積もります。
交換価額から差し引かれるこの金額は、減価償却と呼ばれます。減価償却額はインフレ（不動産の交換費用の増加）によって減少します。通常のメンテナンス; これらの要因が建物の有効年齢を低下させるため、修理（新しい屋根、新しい電気システムなど）。
適用される減価償却額はある程度主観的であり、確かに交渉の対象となります。実際、特定の建物に適用される減価償却額については、多くの場合、意見の相違やある程度の不確実性があります。この現実を考えると、不動産所有者は減価償却の決定を偶然に任せたり、不動産の損失を被るまで待って心配するべきではありません。不動産所有者は、3〜5年ごとに、建物の交換価値と減価償却額の専門家による評価を取得する必要があります。
ACV評価は、特定の建物の修理が必要な場合、または予算の制約によりすべての施設に交換費用ベースで保険をかけることができない場合に、取締役が検討するオプションです。不動産所有者が考慮すべき他の評価オプションもあります。

機能交換費用この評価方法は、以前から利用可能でしたが、広く使用されていません。古い建物を懸念する引受会社が課す不動産保険に現れ始めています。また、機能的に廃止された建物にも使用できます。
この方法では、より安価な材料を使用して、同じ機能を実行する同様のプロパティを持つ建物を置き換えることができます。承認には、建築基準法の自動的な適用範囲が含まれます。
損失が発生した場合、保険会社は4つの支払いオプションのうち最小のものを支払います。
1.全損が発生した場合、保険会社は建物の保険限度額または同じ または異なる）サイトの建物を交換するための費用を 機能的に同等」の支払いで支払うことができます。
2.部分的な損失が発生した場合、保険会社は、同じ建築様式の損傷した部分をより安価な材料（利用可能な場合）で修理または交換するための費用を支払うことができます。
3.保険会社は、建物の損傷していない部分を取り壊し、必要に応じて敷地を片付けるために実際に費やした金額を支払うこともできます。
4. 4番目の支払いオプションは、実際に修理に費やした金額を支払うか、利用可能な場合はより安価な材料を使用して建物を交換することです（Hillman and McCracken1997）。
施設のサービスに使用される特定の備品や動産を除外した交換費用の評価方法とは異なり、この承認は、これらのアイテム（日よけ、床の敷物、電化製品など）の機能的な交換費用の補償を提供します（Hillman nd McCracken1997）。
標準の交換費用価値オプションと同様に、被保険者は物件を修理または交換しないことを選択できます。このような状況では、会社は次のうち最小のものを支払います。
1.責任の限界
2.損失時の 時価」（土地の価値を含まない）。裏書では、 市場価値」とは、公正な市場で売りに出された場合に不動産が実現すると予想される価格と定義しています。」
3. ACVの変更された形式（同じサイトでより安価な材料と同じ建築スタイルで、より少ない減価償却で修理または交換する量）（Hillman and McCracken1997）。
合意された価値または合意された金額合意された価値または合意された金額は、評価方法ではありません。代わりに、彼の用語は、財産保険契約の共同保険条項の放棄を指します。この補償機能の利用可能性は保険会社によって異なりますが、通常、引受人があなたの資産の価値の証明（独立した評価、または保険会社の評価モデルへの準拠）を持っている場合にのみ利用できます。いつ支払いを受けますか？
一般的に、保険会社は、損害または破壊された資産が実際に修理または交換されるまで、損失後合理的に可能な限り早く交換費用の決済を支払いません。
いかなる状況においても、保険会社は、保険の限度額を超えて、またはこの金額が保険の限度額を下回っている場合、損傷した資産の修理または交換に費やした実際の金額を超えて支払うことはありません。
交換費用保険の条件により、被保険者はACVベースで損失を決済することができます。このオプションは、建物を交換する予定がない場合、または交換費用の決済で多額の共同保険ペナルティに直面している場合に行使される可能性があります。

参考資料 :http ://www.schirickinsurance.com/resources/value2005.pdfおよびTIPTON、Harold F.＆KRAUSE、MICKI Information Security Management Handbook、第4版、第1巻、財産保険の概要、587ページ。

最新問題: **255**
Bibaのセキュリティモデルは何に関係していますか？
A. 守秘義務
B. 信頼性
C. 可用性
D. 整合性
Answer: (解答を表示する**)**
Bibaセキュリティモデルは、低いセキュリティレベルのサブジェクトが高いセキュリティレベルのオブジェクトに書き込むことができ、サブジェクトが低いレベルのデータを読み取ることができる場合に、脅威にさらされているデータの整合性に対処します。
出典 :HARRIS、ション、オールインワンCISSP認定試験ガイド、McGraw-Hill / Osborne、2002年、第5章 :セキュリティモデルとアーキテクチャ（ページ244）。

最新問題: **256**
オブジェクトの再利用の概念について正しい説明は次のうちどれですか？
A. オブジェクトの再利用はストレージへの物理的な攻撃から保護します
中くらい。
B. オブジェクトの再利用はリムーバブルメディアにのみ適用されます。
C. オブジェクトの再利用は、オブジェクトへのアクセス権の付与を制御します。
D. オブジェクトの再利用により、ユーザーが残りの情報を取得しないようにします
システムリソースから。
Answer: (解答を表示する**)**
オブジェクトの再利用メカニズムにより、システムリソースが確実に割り当てられ、
の漏洩を防ぐ方法で、許可されたユーザー間で再割り当てされます
機密情報を入手し、システムの許可されたユーザーがシステムリソースから残りの情報を取得しないようにします。オブジェクトの再利用は、ストレージメディアのあるサブジェクトへの再割り当てとして定義されます
（たとえば、ページフレーム、ディスクセクター、磁気テープ）1つ以上のオブジェクトが含まれていました。安全に再割り当てするために、標準のシステムメカニズムを介して新しいサブジェクトが残余データを利用することはできません。7TCSECのオブジェクト再利用要件は、システムリソース、特にストレージメディアが、システムユーザー間で割り当ておよび再割り当てされることを保証することを目的としています。機密情報の開示を防ぐ方法。
答えaは正しくありません。オブジェクトの再利用は必ずしも保護するわけではありません
記憶媒体への物理的な攻撃に対して。回答cも

オブジェクトの再利用は、リムーバブルメディア、固定メディア、実および仮想メインメモリ（レジスタを含む）、キャッシュメモリなど、すべてのプライマリおよびセカンダリストレージメディアに適用されるため、正しくありません。回答dは
承認、ユーザー、プログラム、またはへのアクセス権の付与
処理する。出典：NCSC-TG-018、オブジェクトを理解するためのガイド
信頼できるシステムでの再利用[ライトブルーブック]。

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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: **257**
次のうち、電子メールメッセージの機密性を提供するものはどれですか？
A. 送信者が秘密鍵で暗号化します。
B. 送信者が公開鍵で暗号化します。
C. 送信者は受信者の公開鍵で暗号化します。
D. 送信者は受信者の秘密鍵で暗号化します。
Answer: C (メーッセージを残す**)**
受信者の公開鍵で暗号化すると、メッセージを復号化できるのは受信者だけであるため、電子メールメッセージの機密性は保護されます。送信者は受信者の秘密鍵を持っているとは想定されていません。メッセージをその秘密鍵で暗号化することにより、対応する公開鍵を持っている人は誰でもメッセージを読むことができます。
メッセージを公開鍵で暗号化すると、受信者でさえメッセージを読み取ることができなくなります。
出典：HARRIS、ション、オールインワンCISSP認定試験ガイド、McGraw-Hill / Osborne、2002年、第8章：暗号化517ページ）。

最新問題: **258**
次のうち、情報所有者の責任はどれですか？
A. ユーザーと担当者が情報システム（S）にアクセスするために必要なセキュリティトレーニングを完了していることを確認します
B. 特権やアクセス権を含む情報システム（S）への適切なアクセスを定義する
C. 一般的なセキュリティ管理の識別、実装、および評価の管理
D. 情報システム（S）が合意されたセキュリティ要件に従って運用されていることを確認する
Answer: B (メーッセージを残す**)**

NIST SP 800-18は、情報所有者に対する以下の責任の概要を示しています。これは、データ所有者と同じように解釈できます。
*対象データ/情報の適切な使用と保護のためのルール（行動のルール）を確立します
*情報が存在する情報システムのセキュリティ要件とセキュリティ管理に関する情報を情報システムの所有者に提供します
*誰が情報システムにアクセスできるか、どのような種類の特権またはアクセス権を持っているかを決定します
*情報が存在する一般的なセキュリティ管理策の特定と評価を支援します。

最新問題: **259**
ログオンセッションごとに同じパスワードは？と呼ばれます。
A. 「ワンタイムパスワード」
B. 「2回のパスワード」
C. 静的パスワード
D. 動的パスワード
Answer: C (メーッセージを残す**)**
静的パスワードは、変更されるまで同じままであるパスワードです。これは、オペレーティングシステムで使用するパスワードと同じように設定し、セッション中は常に同じパスワードを使用してシステムにログオンします。
このパスワードは、システムへのアクセスを提供し、特権を取得するためのアクセストークンを正常に作成するための手段になります。ワンタイムパスワードは1回の使用にのみ有効であり、動的パスワードは特定の条件が満たされるたびに変更され、2回パスワードは2回しか使用できません。この種のパスワードを使用して、特定の時間にアクセスできるようにすることができます。

最新問題: **260**
左側の次のセキュリティエンジニアリング用語を右側のBEST定義にドラッグします。

Security Engineering		Definition
Security Risk Treatment		The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the **adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.**
Threat Assessment		A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the **circumstance or event occurs, and the likelihood of occurrence.**
Protection Needs		The method used to identify and characterize the dangers anticipated **throughout the life cycle of the system.**
Risk		The method used to identify feasible security **risk mitigation options and plans.**

ipnpdf.com
(ISC)²®

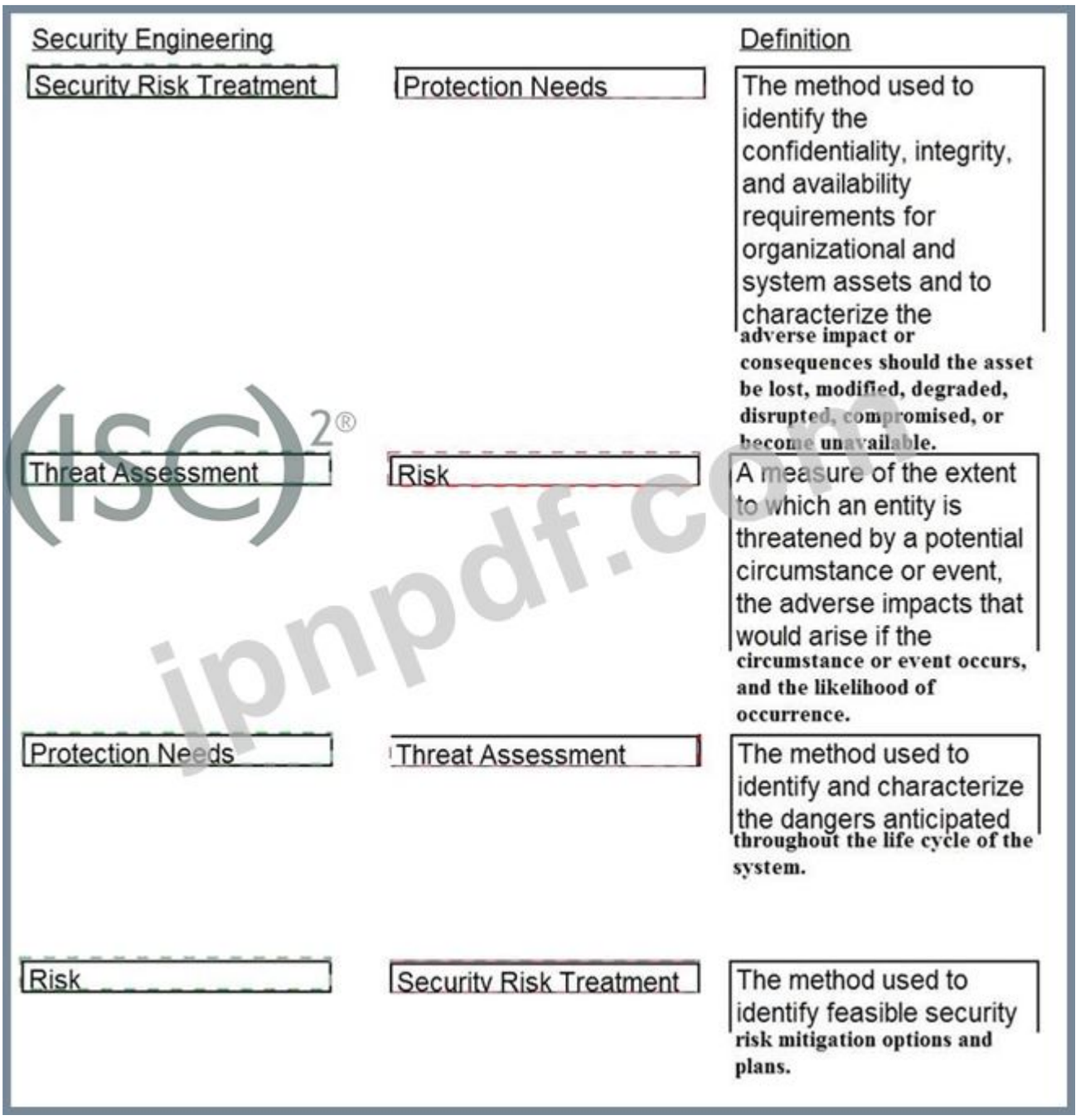
Security Engineering		Definition
Security Risk Treatment		The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the **adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.**
Threat Assessment		A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the **circumstance or event occurs, and the likelihood of occurrence.**
Protection Needs		The method used to identify and characterize the dangers anticipated **throughout the life cycle of the system.**
Risk		The method used to identify feasible security **risk mitigation options and plans.**

ipnpdf.com
(ISC)²®

Answer:

Security Engineering		Definition
Security Risk Treatment	Protection Needs	The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the **adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.**
Threat Assessment	Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the **circumstance or event occurs, and the likelihood of occurrence.**
Protection Needs	Threat Assessment	The method used to identify and characterize the dangers anticipated **throughout the life cycle of the system.**
Risk	Security Risk Treatment	The method used to identify feasible security **risk mitigation options and plans.**

(ISC)2®
jpnpdf.com


Security Engineering
Definition
Security Risk Treatment
Protection Needs
The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.
Threat Assessment
Risk
A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of occurrence.
Protection Needs
Threat Assessment
The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.
Risk
Security Risk Treatment
The method used to identify feasible security risk mitigation options and plans.

説明

	Definition
Protection Needs	The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the **adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.**
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the **circumstance or event occurs, and the likelihood of occurrence.**
Threat Assessment	The method used to identify and characterize the dangers anticipated **throughout the life cycle of the system.**
Security Risk Treatment	The method used to identify feasible security **risk mitigation options and plans.**

(ISC)2®
jpnpdf.com

	Definition
Protection Needs	The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the **adverse impact or consequences should the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.**
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the **circumstance or event occurs, and the likelihood of occurrence.**
Threat Assessment	The method used to identify and characterize the dangers anticipated **throughout the life cycle of the system.**
Security Risk Treatment	The method used to identify feasible security **risk mitigation options and plans.**

(ISC)2®
jpnpdf.com

最新問題: **261**
次のうち、混乱中および混乱後の組織のビジネス機能の維持に焦点を当てているのはどれですか？
A. 事業継続計画
B. 事業回復計画
C. 運用継続計画
D. 災害復旧計画
Answer: A (メーッセージを残す)
事業継続計画（BCP）は、中断中および中断後の組織のビジネス機能の維持に重点を置いています。情報システムは、より大規模なビジネスプロセスへのサポートという観点からのみBCPで考慮されます。事業回復計画（BRP）は、緊急事態後のビジネスプロセスの復旧に対応しています。BRPはBCPに似ていますが、通常、緊急事態または混乱の間、重要なプロセスの継続性を確保するための手順がありません。運用継続計画（COOP）は、代替サイトで組織の重要な機能を復元し、通常の運用に戻る前に最大30日間それらの機能を実行することに重点を置いています。災害復旧計画（DRP）は、通常の施設へのアクセスを長期間拒否する、通常は壊滅的な大規模なイベントに適用されます。DRPは、移転を必要としない軽微な混乱に対処しないという点で、IT緊急時対応計画よりも範囲が狭くなっています。出典：SWANSON、Marianne、et al。、National Institute of Standards and Technology（NIST）、NIST Special Publication 800-34、Contingency Planning Guide for Information Technology Systems、December 2001（page 8）

最新問題: **262**
次のうち、予防的管理ではないものはどれですか？
A. 本番データへのプログラマーアクセスを拒否します。
B. 日付、説明、コスト分析、および予想される効果に関する情報を含めるように変更要求を要求します。
C. 制御と電流源の間のソース比較プログラムを定期的に実行します。
D. 緊急変更の手順を確立します。
Answer: (解答を表示する)
説明/参照：
Explanation:
ソース比較を実行しても、特定のアクションの発生が妨げられることはありません。
セキュリティ管理は、物理的資産、情報、コンピュータシステム、またはその他の資産に対するセキュリティリスクを回避、検出、対抗、または最小化するための保護手段または対策です。コントロールは、資産に対する攻撃を停止、抑止、または減速することにより、損害または損失のリスクを軽減するのに役立ちます。
セキュリティ管理策のレビューまたは設計を支援するために、セキュリティインシデントに関連して、たとえば行動する時間に応じて、いくつかの基準で分類できます。
イベントの前に、予防管理は、たとえばロックすることによってインシデントの発生を防ぐことを目的としています

▪
許可されていない侵入者を排除します。
イベント中、探偵コントロールは進行中のインシデントを特定して特徴づけることを目的としています
▪
たとえば、侵入者の警報を鳴らし、警備員や警察に警告することによって。イベント後、是正管理は、
▪
インシデント。たとえば、組織を可能な限り効率的に通常の作業状態に回復することによって。
不正解：
A :プログラマーが本番データにアクセスできないようにすることは、プログラマーがデータにアクセスできないようにするための予防的制御の一例です。
B：追加情報を含めるように変更要求を行うと、不正な変更が行われるのを防ぐことができます。
D：緊急変更の手順を確立することにより、不正な変更を防ぐことができます。
参照：
https://en.wikipedia.org/wiki/Security_controls

最新問題: **263**
RAIDとは、次のことを指します。
A. 迅速で安価なデジタルテープバックアップ。
B. インターネットドメインのリモート管理。
C. インテリジェントディスクの冗長アレイ。
D. 冗長でフォールトトレラントなインターネットワーキングデバイス。
Answer: C (メーッセージを残す**)**
正解は、インテリジェントディスクの冗長アレイです。他の頭字語は存在しません。

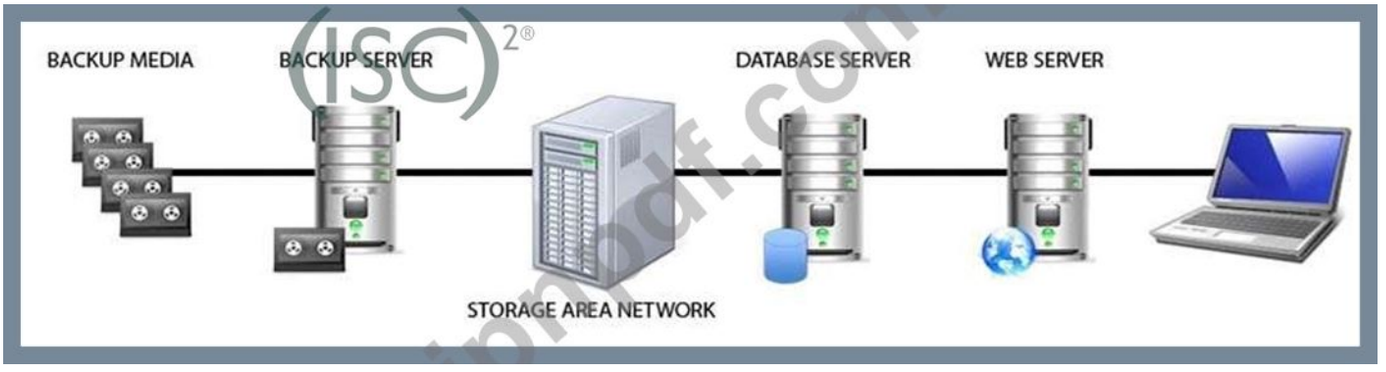
最新問題: **264**
ディザスタリカバリ（DR）テストで、危機管理の特徴となるのは次のうちどれですか？
A. プロセス
B. 戦略的
C. ワイドフォーカス
D. 予想する
Answer: (解答を表示する**)**

最新問題: **265**
大規模な銀行は、オンラインバンキングシステムを使用するすべての顧客にハードウェアトークンを導入しています。トークンは、60秒ごとに6桁の数字のパスワードを生成して表示します。顧客は、この数値のパスワードを使用して銀行口座にログインする必要があります。これはの例です
A. 非同期トークン。
B. 単一要素認証トークン。
C. 同期トークン。

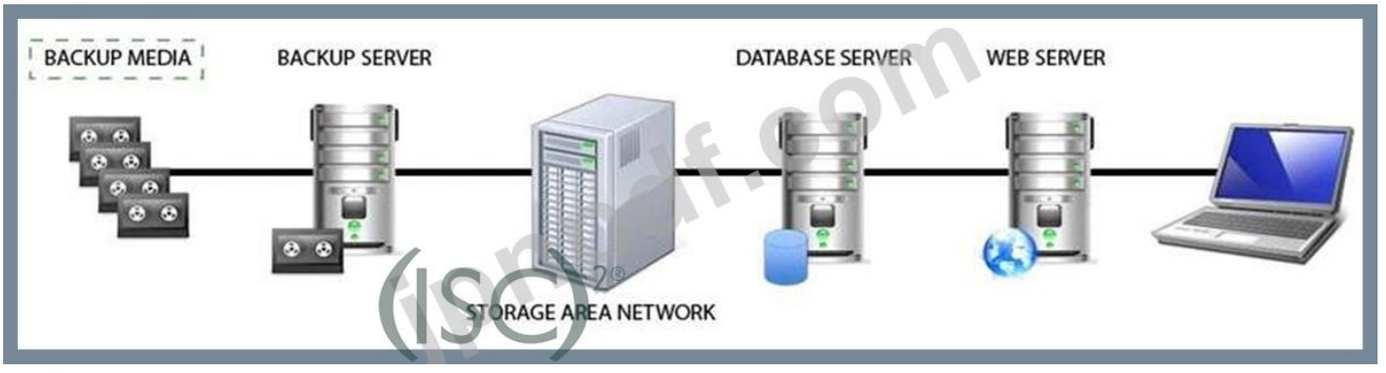
D. シングルサインオン（SSO）トークン。
Answer: C (メーッセージを残す)

最新問題: **266**
セキュリティアーキテクトは、実装のために強制アクセス制御（MAC）モデルを参照することを計画しています。これは、次のプロパティのどれが優先されているかを示していますか？
A. アクセシビリティ
B. 可用性
C. 整合性
D. 守秘義務
Answer: B (メーッセージを残す)

最新問題: **267**
情報アクセスに関連するデジタル説明責任が最も不足している可能性が高いコンポーネントを特定します。
下の画像で正しいデバイスをクリックしてください。



Answer:



説明
バックアップメディア
参照 :CISSP CBKの公式（ISC）2ガイド、第3版1029ページ

最新問題: **268**
フェデレーションID管理（FIM）のアプリケーションプログラミングインターフェイス（API）アクセスを処理するために構築されている承認標準は、次のうちどれですか？
A. ターミナルアクセスコントロールアクセスコントロールシステムプラス（TACACS +）

B. オープン認証（OAUTH）
C. リモート認証ダイヤルインユーザーサービス（RADIUS）
D. セキュリティアサーションマークアップ言語（SAML）
Answer: B (メーッセージを残す**)**

最新問題**: 269**
ソフトウェア開発を開始するときに潜在的なセキュリティ問題に対処するために基本的に必要なものは次のうちどれですか？
A. すべての環境で継続的なセキュリティ監査を実施します。
B. 情報セキュリティの目標を開発に追加します。
C. 開発を本番環境から確実に分離します。
D. 独立したソースコードレビューを実施します。
Answer: B (メーッセージを残す**)**

最新問題**: 270**
財務データと会計データの整合性を保護するため、商用環境で最も一般的に使用されているセキュリティモードはどれですか。
A. Beil-LaPadula
B. クラークウィルソン
C. ビバ
D. グラハムデニング
Answer: B (メーッセージを残す**)**

最新問題**: 271**
ディザスタリカバリプラン（DRP）をテストする主な理由は何ですか？
A. 情報技術（IT）スタッフがそれぞれに割り当てられた役割を認識し、実行することを保証するため
B. バックアップサイトの有効性を検証する
C. 機能しないものを見つけて修正する
D. 情報技術（IT）スタッフの間で高レベルのDRP認識を作成する
Answer: B (メーッセージを残す**)**
セクション :セキュリティの評価とテスト
説明

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

こちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (1533**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: **272**
ISC2によると、情報処理施設の壁の耐火性はどうあるべきですか？
A. すべての壁の最低耐火性は2時間である必要があります
B. すべての壁の最低耐火性は1時間である必要があります
C. 紙やメディアなどの記録が保管されている隣接する部屋の壁を除き、すべての壁の最低耐火性は1時間である必要があります。ただし、紙やメディアなどの記録は最低2時間の耐火性である必要があります。
D. 紙やメディアなどの記録が保管されている隣接する部屋の壁を除き、すべての壁の最低耐火性は2時間である必要があり、最低耐火性は3時間である必要があります。
Answer: (解答を表示する**)**

最新問題: **273**
個人がインターネット接続をプライベートに保つためにすべての手順を実行したと仮定すると、次のうちどれがプライベートにWebを閲覧するのに最適ですか？
A. 閲覧アクティビティファームに関する情報が個人用デバイスに保存されないようにします。
B. ブラウジングアクティビティに関する情報がクラウドに保存されないようにします。
C. 個人のデバイスでのブラウジングアクティビティに関する情報を保存します。
D. ブラウジングアクティビティをクラウドに保存します。
Answer: (解答を表示する**)**

最新問題: **274**
システムに複数の情報所有者からのデータが含まれている場合、各情報所有者は何をしなければなりませんか？
A. データのセキュリティ要件に関して情報システム（IS）の所有者に情報を提供します
B. 情報システム（IS）のセキュリティ評価レポート（SAR）を確認し、ISの運用を承認します。
C. データを含む情報システム（IS）のシステムセキュリティ計画（SSP）を作成し、維持します
D. 他の情報所有者が所有するデータを含まない情報システム（IS）にデータを移動します
Answer: C (メーッセージを残す**)**
セクション :セキュリティの評価とテスト

最新問題: **275**
Rijndaelブロック暗号アルゴリズムに関する次のうちどれが間違っていますか？
A. Rijndaelの設計は、ブロック暗号Squareの設計に強く影響されました。
B. キー長とブロック長の合計25の組み合わせが可能です
C. ブロックサイズとキー長の両方を64ビットの倍数に拡張できます。
D. 暗号のブロック長とキー長は可変です。
Answer: C (メーッセージを残す**)**

上記の答えはFALSEであるため、正解です。Rijndaelは、64ビットの倍数をサポートしていませんが、128ビットから256ビットの範囲の32ビットの倍数をサポートしています。キーの長さは、128、160、192、224、および256にすることができます。
ブロック長とキー長の両方を、32ビットの倍数に非常に簡単に拡張できます。可能な25の異なるブロックとキーサイズの合計の組み合わせ。
Rijndael Cipher Rijndaelは、アメリカ合衆国のAdvanced Encryption Standard（AES）の候補アルゴリズムとして、JoanDaemenとVincentRijmenによって設計されたブロック暗号です。暗号のブロック長とキー長は可変です。
Rijndaelは、さまざまなプロセッサとハードウェアに非常に効率的に実装できます。Rijndaelの設計は、ブロック暗号Squareの設計に強く影響されました。
Advanced Encryption Standard（AES）
Advanced Encryption Standard（AES）キーは、AESの要件に従って、128、192、または256ビットのいずれかに定義されています。
ラウンド数、つまりメインアルゴリズムの反復回数は、Advanced Encryption Standard（AES）内で10から14まで変化する可能性があり、ブロックサイズとキーの長さに依存します。128ビットキーは10ラウンドまたは暗号化を使用し、192ビットキーは12ラウンドの暗号化を使用し、256ビットキーは14ラウンドの暗号化を使用します。
ラウンド数の少なさはRijndaelの主な批判の1つですが、これが問題になった場合は、ブロックサイズとキーの長さを増やすことで、パフォーマンスの面でわずかな追加コストでラウンド数を簡単に増やすことができます。
RijndaelとAESのキーとブロックの長さの範囲RijndaelとAESは、ブロック長と暗号化キーの長さでサポートされている値の範囲のみが異なります。
Rijndaelの場合、ブロック長とキー長は、最小128ビット、最大256ビットの32ビットの倍数に個別に指定できます。ブロックおよびキーの長さ160および224ビットのサポートは、JoanDaemenおよびVincentRijmen、RijndaelのAES提出ドキュメント、バージョン2、1999年9月に導入されました。http ://csrc.nist.gov/archive/aes/rijndael/Rijndaelで入手できます。-ammended.pdf
AESは、ブロック長を128ビットに固定し、128、192、または256ビットのキー長のみをサポートします。
この質問に使用される参照 :Rijndaelページおよび
http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdfおよびFIPS PUB 197、Advanced Encryption Standard（AES）、米国国立標準技術研究所、米国商務省、2001年11月。

最新問題**: 276**
継続性戦略を定義するために必要な情報に関して、以下のどの選択肢が最も正確ですか？該当するものをすべて選択。
A. 戦略は、破壊的なイベント中の施設の使用に対処する必要があります。
B. コンピューティング要素を維持するために、戦略を定義する必要があります。
ハードウェア、ソフトウェア、およびネットワーク要素として。
C. 他の選択肢はありません。

D. 戦略では、継続性の実装における人員の役割を定義する必要があります。
Answer: A,B,D (メーッセージを残す)

最新問題: **277**
以下のどの選択肢がメディアコントロールの例ではありませんか？
A. 安全な部屋のプリンターへの印刷
B. 個人の身元調査を実施する
C. 廃棄前にメディアを消毒する
D. バックアップメディアのコピーを物理的に保護する
Answer: B (メーッセージを残す)
答えは人事管理です。ほとんどのサポートと操作
スタッフはシステムに特別にアクセスできます。一部の組織は
スクリーニングのためにこれらのポジションを埋める個人の身元調査
おそらく信頼できない個人を排除します。
*回答 「廃棄前にメディアをサニタイズする」：廃棄前にメディアから情報を削除するプロセスは、サニタイズと呼ばれます。メディアのサニタイズには、上書き、消磁、破壊の3つの手法が一般的に使用されます。
※回答 「安全な部屋のプリンターへの印刷」：共用部の汎用プリンターではなく、鍵のかかった部屋のプリンターへの印刷など、実際に安全な場所のメディアにデータを出力する必要がある場合があります。範囲。
*回答 「バックアップメディアのコピーを物理的に保護する」：オフサイトに保存されているバックアップメディアのコピーの物理的保護には、オンサイトに保存されている同じ情報を含むメディアと同等の保護レベルを与える必要があります。
出典：米国国立標準技術研究所 コンピュータセキュリティの概要：NISTハンドブック特別刊行物800-12。

最新問題: **278**
TCSECレーティングのB3レベルで、コンピューターベースの情報システムにユーザークリアランスを実装する責任は誰にありますか？
A. セキュリティ管理者
B. 演算子
C. データ所有者
D. データ管理者
Answer: A (メーッセージを残す)
セキュリティ管理者機能には、ユーザークリアランスの設定、初期パスワードの設定、新規ユーザーのその他のセキュリティ特性の設定、既存ユーザーのセキュリティプロファイルの変更などのユーザー指向のアクティビティが含まれます。データ所有者は、データを保護する最終的な責任を負い、データへの適切なユーザーアクセス権を決定します。出典：TIPTON、Hal、（ISC）2、CISSP試験プレゼンテーションの概要。

最新問題: **279**
データベースビューは何に使用されますか？
A. 参照整合性を確保するため。
B. データベース内のデータに簡単にアクセスできるようにするため。
C. データベース内のデータへのユーザーアクセスを制限します。
D. 監査証跡を提供します。
Answer: (解答を表示する**)**
ビューを使用することで、特定のデータまたはデータベース内の情報を含む実際のテーブルへのユーザーアクセスを制限する組織にセキュリティを提供できます。たとえば、3つのテーブルからのデータを表示するビューを作成できます。
それぞれの4つの列のうちの2つ。情報を含むテーブルへのアクセスを許可する代わりに、ビューへのアクセスを許可します。これにより、ユーザーはこの固定情報にアクセスできますが、それを含むテーブルに対する特権はありません。これにより、セキュリティが提供されます。

最新問題: **280**
「ポートノッキング」テクノロジーを利用したいと考えています。これをどのように説明できますか？
A. ポートノッキングは、クライアントが事前定義されたポートのセットに接続して、許可されたクライアントとして識別しようとする場所です。
B. ポートノッキングとは、ユーザーがサーバーオペレーターに電話をかけて、接続したいサービスを開始させることです。
C. これは、サーバー上ですべてのポートが開いている場所であり、接続しているクライアントは、接続したい開いているポートをスキャンして、開いていて実行されているかどうかを確認します。
D. ポートノッキングとは、ポートシーケンスが3DESで暗号化され、サーバーだけがポートシーケンスを復号化するための他のキーを持っている場合です。
Answer: A (メーッセージを残す**)**
説明/参照：
Explanation:
ポートノッキングは、ファイアウォールの背後にあるコンピューターやその他のネットワークデバイスへのアクセスを制御するためにネットワーク管理者が使用する認証方法です。ポートノッキングはファイアウォールルールを利用して、「シークレットノック」を知っているクライアントが一連の接続試行（ノックシーケンスと呼ばれる）を実行することにより、特定のポートを介してネットワークに入ることができるようにします。特定のポートの正しいノックシーケンスは、ネットワーク管理者によって特定のIPアドレスに対して作成されます。デーモンと呼ばれる小さなプログラムは、ファイアウォールのログファイルで接続要求を監視し、ネットワークを探しているクライアントが承認されたIPアドレスのリストにあり、正しいノックシーケンスを実行したかどうかを判断します。答えが「はい」の場合、関連するポートを開き、アクセスを許可します。もちろん、許可されていない人がノックシーケンスを発見した場合、

不正解：
B :ポートノッキングは、ユーザーがサーバーオペレーターに電話して、接続したいサービスを開始させる場所ではありません。
C :ポートノッキングは、サーバー上ですべてのポートが開いている場所ではなく、接続しているクライアントは、接続したい開いているポートをスキャンして、開いていて実行されているかどうかを確認します。
D :ポートノッキングは、ポートシーケンスが3DESで暗号化されている場所ではなく、サーバーだけがポートシーケンスを復号化するための他のキーを持っています。
参照：
http://whatis.techtarget.com/definition/port-knocking
http://www.portknocking.org/

最新問題**: 281**
以下のどの選択肢がその人の役割または責任です
緊急時対応計画プロセスを管理するように指定されていますか？3つ選択してください
A. 上級管理職に指示を与える
B. すべての重要なビジネス機能の識別を確実にする
C. ビジネスユニット間で計画プロセスを統合する
D. イベント後の従業員へのストレス軽減プログラムの提供
Answer: A,B,C (メーッセージを残す**)**
緊急時対応計画担当者は、事業継続、災害復旧、緊急管理、または事業再開プロセスを計画する際に多くの役割と責任を負います。正解に加えて、これらの役割と責任の一部には次のものが含まれます。緊急時対応計画プログラムへの経営幹部のコンプライアンスの確保定期的な管理レポートとステータスの提供緊急対応組織の活性化の調整と統合回答 Dイベント後の従業員へのストレス軽減プログラムの提供」、イベント後に従業員にストレス軽減プログラムを提供することは、人材分野の責任です。出典：緊急時対応計画と管理、緊急時対応計画101、Kelley Goggins、1999年3月。

最新問題**: 282**
ニューラルネットワークとは何ですか？
A. 人工知能タスクを実行する一連のネットワーク化されたPC
B. 生物学的ニューロンの機能をエミュレートするハードウェアまたはソフトウェアシステム
C. 医療アプリケーションに焦点を当てたコンピューターのコレクション
D. 人間の専門家の推論をエミュレートするハードウェアまたはソフトウェアシステム
Answer: B (メーッセージを残す**)**
ニューラルネットワークはハードウェアまたはソフトウェアです
生物学的ニューロンの機能をエミュレートするシステム。
回答 人間の専門家の推論をエミュレートするハードウェアまたはソフトウェアシステム」とは、エキスパートシステム。他の答えは気を散らすものです。

最新問題: **283**
次のプロトコルのどれがネイティブ暗号化を提供しますか？
A. IPSEC、SSH、PPTP、SSL、MPLS、L2F、およびL2TP
B. IPSEC、SSH、SSL、TFTP
C. IPSEC、SSH、SSL、TLS
D. IPSEC、SSH、PPTP、SSL、MPLS、およびL2TP
Answer: C (メーッセージを残す**)**
次の答えは正しくありません。
L2TPおよびPPTPは提供しないため、IPSEC、SSH、PPTP、SSL、MPLS、およびL2TPは正しくありません。
暗号化。
TFTPは暗号化を提供しないため、IPSEC、SSH、SSL、TFTPは正しくありません。
IPSEC、SSH、PPTP、SSL、MPLS、L2F、およびL2TPは正しくありません。これは、MPLS、L2F、およびL2TPが正しくないためです。
暗号化を提供しません。
ノート：
PPTPは暗号化をネイティブに提供しませんでした。暗号化を提供するのはMicrosoftのMPPEです。
MPPEは、ポイントツーポイントリンクを暗号化するためにMicrosoftによって開発された暗号化テクノロジです。これらは
PPP接続は、ダイヤルアップ回線またはVPNトンネルを介して行うことができます。MPPEはのサブ機能として機能します
Microsoftポイントツーポイント圧縮（MPPC）。
MPPCは、クライアントデバイス間でPPPパケットを圧縮するために使用されるスキームです。MPPCアルゴリズム
複数の同時サポートをサポートするために帯域幅使用率を最適化するように設計されています接続。
MPPEは、圧縮制御プロトコル（CCP）内のMPPCオプションのビットを使用してネゴシエートされます。
MPPC構成オプション（CCP構成オプション番号18）。
MPPEは、40ビットまたは128ビットのキーでRC4アルゴリズムを使用します。すべてのキーは、ユーザーのクリアテキスト認証パスワード。RC4はストリーム暗号です。したがって、のサイズ暗号化および復号化されたフレームは、元のフレームと同じサイズです。シスコ
MPPEの実装は、Microsoftの実装と完全に相互運用可能であり、利用可能なすべてのオプションを使用します。
ヒストリーレスモードを含みます。履歴のないモードは、次のような損失の多い環境でスループットを向上させることができます
どちらの側も暗号化を同期するためにCCPリセット要求を送信する必要がないため、VPNとしてパケットが失われたときのコンテキスト。

この質問を作成するために、次の参照が使用されました。
CISSP CBKの公式（ISC）2ガイド、第3版、874および355ページ（IPSEC）、360（SSH）、
359（PPTP）、362（SSL）、361（SOCKS）、360（L2TP）。
と
http://www.cisco.com/en/US/products/ps6587/products_white_paper09186a008019bf38.shtml#15190

最新問題: **284**
次の回答のうち、データバックアップ計画の最も重要な部分を最もよく示しているのはどれですか？
A. 復元操作を使用したバックアップのテスト
B. 効果的なバックアップ計画
C. 信頼性の高いネットワークインフラストラクチャ
D. 高価なバックアップハードウェア
Answer: (解答を表示する**)**
バックアップシステムから失われたファイルを復元できない場合、バックアップ計画は役に立ちません。最高のバックアップシステムと計画を利用できる可能性がありますが、ファイルを復元できない場合、システムはデータの可用性を保証できません。
効果的なディザスタリカバリ計画を作成し、その計画に組織のニーズを満たす優れたバックアップ戦略を含めます。システムの有効性を証明するために、定期的な復旧作業を必ず含めてください。
次の答えは正しくありません。
-効果的なバックアップ計画 :これは不可欠ですが、ネットワークを安全に運用するには、復元を使用して計画をテストすることが不可欠です。
-信頼性の高いネットワークインフラストラクチャ :これは、効果的なバックアップと復元の計画を立てるために必要なものの一部にすぎないため、正しくありません。
-高価なバックアップハードウェア :これは便利ですが、復元計画を立てずに、必要なときに機能しない場合は、役に立ちません。
この質問を作成するために、次の参照が使用されました :2013.公式セキュリティ+カリキュラム。

最新問題: **285**
質問に答えるには、以下の情報を参照してください。
組織内のデスクトップコンピューターは、同等のセキュリティ環境で再利用できるようにサニタイズされました。データは組織のポリシーに従って破棄され、以前は磁気ドライブに保存されていたデータの機密性に関するすべてのマーキングおよびその他の外部表示が削除されました。
組織のポリシーでは、携帯情報端末からユーザーデータを削除する必要があります
（PDA）デバイスを廃棄する前に。デバイスが誤動作している場合、ユーザーデータを削除できない場合があります。以下のどの破壊方法が、データが削除されたことを最もよく保証しますか？
A. 消磁
B. ローレット

C. 粉砕
D. 細断
Answer: D (メーッセージを残す**)**

最新問題**: 286**
データ暗号化標準（DES）暗号化アルゴリズムには、次のどの特性がありますか？
A. 64ビットのデータ入力は56ビットの暗号化された出力になります
B. パリティに使用される8ビットの128ビットキー
C. 合計キー長が64ビットの64ビットブロック
D. 56ビットのデータ入力は56ビットの暗号化された出力になります
Answer: C (メーッセージを残す**)**
説明/参照：
Explanation:
DESは、対称ブロック暗号化アルゴリズムです。平文の64ビットブロックが入ると、暗号文の64ビットブロックが出てきます。これは対称アルゴリズムでもあり、暗号化と復号化に同じキーが使用されることを意味します。64ビットキーを使用します。56ビットが真のキーを構成し、8ビットがパリティに使用されます。
DESアルゴリズムがデータに適用されると、メッセージがブロックに分割され、一度に1つずつ操作されます。ブロックは、16ラウンドの転置および置換関数を通過します。転置および置換関数の順序とタイプは、アルゴリズムで使用されるキーの値によって異なります。結果は、暗号文の64ビットブロックです。不正解：
A：平文の64ビットブロックが入ると、暗号化されたデータの64ビットブロックが出てきます。
B：DESは64ビットキー（128ビットではない）を使用します。56ビットが真のキーを構成し、8ビットがパリティに使用されます。
D：DESは56ビットではなく64ビットブロックを使用します。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、2013、p。801

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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**: 287**
情報システム（IS）内の情報について誰が責任を負いますか？
A. セキュリティマネージャー
B. システム所有者

C. データ所有者
D. データプロセッサ
Answer: C (メーッセージを残す**)**
セクション :セキュリティ運用

最新問題**: 288**
どのオレンジブックの評価レベルが 検証済みの設計」として説明されていますか？
A. A1。
B. B3。
C. B2。
D. B1。
Answer: (解答を表示する**)**
レベルA1は、検証済み設計として説明されています。
次の答えは正しくありません。
B3。レベルB3はセキュリティドメインとして記述されているため、これは正しくありません。
B2。レベルB2は構造化保護として記述されているため、これは正しくありません。
B1。レベルB1はラベル付きセキュリティとして記述されているため、これは正しくありません。

最新問題**: 289**
次のうち、一般的に対象と見なされないものはどれですか
HIPAA法のタイトルII、管理の簡素化に基づくエンティティ？
A. 雇用主
B. 健康情報を送信する医療提供者
標準的なトランザクションに関連して電子的に
C. 健康保険
D. ヘルスケアクリアリングハウス
Answer: (解答を表示する**)**
雇用主はHIPAaの対象外です。HIPAA
医療情報を送信する医療提供者に適用されます
電子形式、ヘルスケアクリアリングハウス、およびヘルスプラン。ただし、一部の雇用主はグラム・リーチ・ブライリーの対象となる場合があります
活動。グラム・リーチ・ブライリー（GLB）法は、11月12日に制定されました。
1999年、特定の事業活動、合併、および提携を制限していた銀行に対する大恐慌時代の制限を撤廃する。グラス・スティーガル法第20条および第32条に含まれる証券会社と提携している銀行に対する制限を撤廃します。GLBは11月に発効しました
2001年13月13日。GLBはまた、電子およびその他の形式の会員および加入者データを保護するために健康保険および保険会社を要求しています。これらの健康保険および保険会社は、次のような新しい州法および規制に該当します。
GLBが明示的に割り当てるため、GLBを実装するために渡されます

州の保険当局に対する健康保険および保険会社の規制の施行（15 USc。b6805）。Gramm-Leach-Blileyのプライバシーとセキュリティの要件の一部は、HIPAAの要件と類似しています。
ほとんどの州は、健康保険と保険会社が
2001年7月1日までのGLB要件、および金融機関は
これにより、グラム・リーチ・ブライリーに完全に準拠する必要があります
日にち。他の回答は、
HIPAA規制。

最新問題: **290**
以下のどのステートメントが違いを最も正確に説明していますか
セキュリティ意識、セキュリティトレーニング、セキュリティ教育の間？
A. すべてのシステムオペレーターにセキュリティ教育が必要です。
B. セキュリティトレーニングはセキュリティ教育よりも詳細です。
C. セキュリティトレーニングは、従業員が
より安全に仕事を遂行します。
D. 上級管理職にはセキュリティ意識は必要ありません。
Answer: C (メーッセージを残す**)**
意識は、セキュリティが
貴重な資源を保護することによる組織の使命。The
トレーニングの目的は、人々がより安全に仕事を遂行できるようにするスキルを教えることです。セキュリティ教育はセキュリティトレーニングよりも詳細であり、セキュリティの専門家やセキュリティの専門知識が必要な仕事をしている人を対象としています。プログラムの開発と実装に使用されるリソースのため、またプログラムが影響を与えるため、経営陣のコミットメントが必要です。
彼らのスタッフ。出典：米国国立標準技術研究所
コンピュータセキュリティ入門 :NISTハンドブック特別刊行物–
800-12。

最新問題: **291**
質問に答えるには、以下の情報を参照してください。
マルチレベルセキュリティ（MLS）システムでは、次の機密ラベルが機密レベルの増加に使用されます：制限付き、機密、秘密、極秘。表Aに4人のユーザーのクリアランスレベルを示し、表Bに4つの異なるファイルのセキュリティクラスを示します。

Table A

User	Clearance Level
A	Restricted
B	Confidential
C	Secret
D	Top Secret

Table B

Files	Security Class
1	Restricted
2	Confidential
3	Secret
4	Top Secret

(ISC)2 pdf.com

Bell-LaPadulaシステムでは、4つのファイルのいずれかにデータを書き込むときに最も制限のあるユーザーはどれですか。
A. ユーザーD
B. ユーザーC
C. ユーザーA
D. ユーザーB
Answer: A (メーッセージを残す**)**

最新問題**: 292**
情報処理施設を運営することを目的としたオフサイトのバックアップ施設で、コンピューターや通信機器はありませんが、フローリング、電気書き込み、エアコンなどがあります。
A. ホットサイト
B. 重複処理機能
C. コールドサイト
D. ウォームサイト
Answer: (解答を表示する**)**
コールドサイトには、ハードウェアをインストールしてコンピュータ環境を再現できるようにするための適切な電力要件と床面積がすべてありますが、実際の機器は提供されません。ホットサイトを提供する企業の多くは、コールドサイトも提供しています。あなたの会社がホームサイト以外の場所で利用可能なフロアスペースを持っている場合、あなたの会社が勝ったコールドサイトを作成することを検討することは合理的かもしれません。操作を復元するには、ホットサイトよりもはるかに多くの停止が必要です。

最新問題**: 293**
次のうち、暗号化アルゴリズムではないものはどれですか？
A. スキップジャック
B. SHA-1
C. Twofish
D. DEA
Answer: B (メーッセージを残す**)**
SHA-1は、暗号化アルゴリズムとは対照的なハッシュアルゴリズムです。参照 :293ページTittel：CISSP学習ガイド

最新問題**: 294**
認定および認定するための標準的なプロセス
A. DIACAP
B. DITSCAP
C. CIAP
D. NIACAP
Answer: B (メーッセージを残す**)**

正解は、防衛情報技術セキュリティであるDITSCAPです。
認証および認定プロセス。
*回答NIACAPは、米国政府の非防衛認証を指し、
認定（C&A）は、国家情報保証認証を処理し、
認定プロセス。
* CIAPは、商用システムに適用するために現在開発中の商用情報セキュリティ分析プロセスを指します。
*回答DIACAPは気を散らすものです。

最新問題: **295**
IANAによって登録された「Registerports」はどのポートですか？
A. ポート128～255
B. ポート1024～49151
C. ポート1023～65535
D. ポート1024～32767
Answer: B (メーッセージを残す**)**
* 0-1023（IANAによって割り当てられた）のシステムポート（既知のポートとも呼ばれます）
*ユーザーポート（登録ポートとも呼ばれます）、1024～49151（IANAによって割り当てられています）
* 49152～65535 のダイナミックポート（プライベートポートまたはエフェメラルポートとも呼ばれます）（割当てられていません）
参照：http ://tools.ietf.org/html/draft-ietf-tsvwg-iana-ports-10

最新問題: **296**
オブジェクト指向データベース（OODB）システム：
A. 画像やグラフィックスなどの複雑なデータの保存と操作に役立ちます。
B. 最小限のシステムリソースを消費します。
C. テキストのみの情報に最適です。
D. プログラマーに必要な学習時間は最小限です。
Answer: A (メーッセージを残す**)**
正解は、「画像や画像などの複雑なデータの保存と操作に役立ちます。
グラフィックス」。他の答えは誤りです。なぜなら、答えは「テキストのみに理想的に適している」からです。
情報」リレーショナルデータベースは、テキストのみの情報に最適です。
「プログラマーに最小限の学習時間を要求する」および「最小限のシステムリソースを消費する」。
OODBシステムは学習曲線が急で、大量のシステムリソースを消費します。

最新問題: **297**
セキュリティポリシーとは何ですか？

A. セキュリティに関して満たさなければならない経営陣の期待に関するハイレベルな声明
B. ネットワークへの認証を定義するポリシー。
C. 安全な姿勢を確保することに重点を置き、経営陣の承認を表明する方針。要件を実装する方法について詳しく説明します。
D. システムの承認プロセスに焦点を当てたステートメント
Answer: (解答を表示する**)**
準拠していると見なされるために満たされなければならない期待に関する声明。これは、ポリシーが、組織に対するセキュリティの期待を表現するために経営陣が承認し、遅れをとっている幅広い声明であるためです。
次の答えは正しくありません。
承認はセキュリティポリシーを満たすための重要な要素である可能性がありますが、それだけが焦点ではないため、システムの承認プロセスに焦点を当てたステートメントは正しくありません。
ネットワークへの認証はセキュリティ上の懸念全体の1つの側面にすぎないため、ネットワークへの認証を定義するポリシーは正しくありません。ポリシーは、ネットワーク以上のものと認証以上のものにも焦点を当てる必要があります。
安全な姿勢を確保することに重点を置き、経営陣の承認を表明する方針。
「詳細説明」の部分が原因で、要件の実装方法が正しくないことを詳細に説明しています。ポリシーはステートメントであり、詳細は扱いません。
この質問を作成するために、次の参照が使用されました。
ション・ハリス、最新のオールインワンスCISSP試験準備p227; また、ISC2公式ガイドCISSP試験、p82

最新問題**: 298**
レコード破棄要件がデータ保持ポリシーに含まれている理由を説明しているのは次のうちどれですか？
A. 法的要件およびビジネス要件に準拠するため
B. データの所有権を検証する
C. ストレージとバックアップのコストを節約するため
D. 破壊ガイドラインを満たすため
Answer: A (メーッセージを残す**)**

最新問題**: 299**
ロールベースアクセス制御（RBAC）のコアコンポーネントは、定義されたデータ要素で構成する必要があります。どの要素が必要ですか？
A. 役割、操作、アカウント、および保護されたオブジェクト
B. ユーザー、権限、オペレーター、および保護されたオブジェクト
C. 役割、アカウント、権限、および保護されたオブジェクト
D. ユーザー、ロート、操作、および保護されたオブジェクト

Answer: (解答を表示する)

最新問題: **300**
ユーザーIDを検証するためにどのような種類の証明書が使用されますか？
A. 公開鍵証明書
B. 属性証明書
C. ルート証明書
D. コード署名証明書
Answer: (解答を表示する)
暗号化では、公開鍵証明書（またはID証明書）は、デジタル署名を組み込んだ電子文書であり、公開鍵とID（個人または組織の名前、住所などの情報）を結び付けます。証明書を使用して、公開鍵が個人に属していることを確認できます。
一般的な公開鍵インフラストラクチャ（PKI）スキームでは、署名は認証局（CA）のものになります。Web of Trustスキームでは、署名はユーザー（自己署名証明書または他のユーザー（「承認」）のいずれかです。いずれの場合も、証明書の署名は、ID情報と公開鍵が一緒に属していることを示す証明書署名者による証明です。
コンピュータセキュリティでは、認証証明書（属性証明書とも呼ばれます）は、発行者が制御する、または使用するためのアクセス権を持つサービスまたはリソースを使用するための発行者からの書面による許可を説明するデジタルドキュメントです。権限を委任することができます。
PKCとACを常に混同している人もいます。類推によって区別が明確になる場合があります。PKCはパスポートのようなものと見なすことができます。PKCは所有者を識別し、長期間使用する傾向があり、簡単に入手することはできません。ACは入国ビザのようなものです。通常、ACは別の機関によって発行され、長期間は持続しません。入国ビザを取得するには通常パスポートを提示する必要があるため、ビザの取得はより簡単なプロセスになる可能性があります。
この実際の例は、大規模なサービスプロバイダーによるモバイルソフトウェアの展開に見られ、通常、Microsoftスマートフォン（および関連）、Symbian OS、J2MEなどのプラットフォームに適用されます。
これらの各システムでは、モバイル通信サービスプロバイダーは、モバイル端末クライアントの配布（つまり、携帯電話のオペレーティングシステムまたはアプリケーション環境）をカスタマイズして、「ファームウェアの更新」などの一連の機能またはアクセス許可にそれぞれ関連付けられた1つ以上のルート証明書を含めることができます。「連絡先名簿へのアクセス」、「無線インターフェースの使用」、そして最も基本的なもの、「インストールして実行」。開発者がこれらの制御された環境の1つで配布と実行を有効にする場合は、適切なCA（通常は大規模な商用CA）から証明書を取得する必要があります。その過程で、通常、次のような帯域外メカニズムを使用してIDを検証します。電話、政府および商業データベースを介した法人の検証などの組み合わせ、
IDが検証されると、ソフトウェアへの署名に使用できるID証明書が発行されます。通常、開発者または発行者のID証明書によって署名されたソフトウェアは配布されませんが、特定のソフトウェアリリースに固有の認証証明書を生成する前に、コンテンツをテストまたはプロファイリングするためにプロセッサに送信されます。次に、その証明書は、配布の準備の最後のステップとしてソ

フトウェアに署名するために、一時的な非対称キーペアとともに使用されます。ID証明書と認証証明書を分離することには、特にシステムに受け入れられる新しいコンテンツのリスク軽減とキー管理、および攻撃ベクトルとして使用される可能性のある誤ったソフトウェアからの回復に関連する多くの利点があります。
参照：
HARRIS、ション、オールインワンCISSP認定試験ガイド、2001年、McGraw-Hill / Osborne、540ページ。
http://en.wikipedia.org/wiki/Attribute_certificate
http://en.wikipedia.org/wiki/Public_key_certificate

最新問題: **301**
組織内の誰がデータ情報資産の分類に責任を負いますか？
A. データアーキテクト
B. 最高情報責任者（CIO）
C. 最高情報セキュリティ責任者（CISO）
D. データ所有者
Answer: (解答を表示する**)**

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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: **302**
次の問題のうち、Kerberosで対処されていないものはどれですか？
A. 可用性
B. 守秘義務
C. 整合性
D. 認証
Answer: A (メーッセージを残す**)**
説明/参照：
Explanation:
Kerberosは、MITのProjectAthenaの下で開発された信頼できるサードパーティの認証プロトコルです。
ギリシャ神話では、Kerberosは冥界への入り口を守る3頭の犬です。Kerberosは、対称鍵暗号を使用して、クライアントがサービスを必要とするネットワーク上の他のエンティティに対してクライアントを認証します。

Kerberosは、情報の機密性と整合性に対応しています。可用性については触れていません。
不正解：
B :Kerberosは機密性に対処します。
C :Kerberosは整合性をアドレス指定します。
D :Kerberosはアドレス認証を行います。
参照：
Krutz、RonaldL.およびRussellDean Vines、CISSPおよびCAP準備ガイド :CISSPおよびCAPの習得、Wiley Publishing、インディアナポリス、2007年、p。78

最新問題: **303**
階層型PKIでは、最高のCAは通常ルートCAと呼ばれますが、次の用語のどれによっても参照されますか？
A. 下位CA
B. トップレベルのCA
C. ビッグCA
D. マスターCA
Answer: B (メーッセージを残す**)**
参照 :Arsenault、Turner、Internet X.509公開鍵インフラストラクチャ :ロードマップ、章"用語"。
また、認証局アンカー (CAA)などの他の用語が一部の政府組織内で使用される場合があることにも注意してください。トップレベルCAは、トップレベルCAを示す別の一般的な用語であり、トップレベルアンカーも使用できます。

最新問題: **304**
次のうち、プロトタイピングの利点はどれですか？
A. プロトタイプシステムは、時間とコストを大幅に節約できます。
B. プロトタイプシステムでは、変更管理はそれほど複雑ではないことがよくあります。
C. 目的のシステムに機能や追加機能が追加されないようにします。
D. 強力な内部統制は実装が容易です。
Answer: A (メーッセージを残す**)**
プロトタイプフェーズは、 概念実証」フェーズとも呼ばれます。
それがどちらと呼ばれるかは、作成者が 証明」しようとしているものによって異なります。
フェーズの主な成果物に製品の技術的機能の作業バージョンが含まれている場合、それは プロトタイプ」です。主な成果物が製品の技術的特徴を備えているように見える場合、それは 概念実証」です。
プロトタイプは、プロセスの早い段階でいくつかの機能をテストできるため、時間とお金を節約できます。テストを開始するために、最終製品全体を作成する必要はありません。

最新問題: **305**

次のアサーションのうち、侵入検知でのパターンマッチングと異常検出について正しくないものはどれですか？
A. 異常検出はより多くのデータを生成する傾向があります
B. IDSに一致するパターンは、既知の攻撃のみを識別できます
C. トラフィックストリームの代わりに個々のパケットを分析することにより、攻撃シグネチャのステートフルマッチングスキャン
D. 異常ベースのエンジンは、通常のトラフィックアクティビティとスループットのベースラインを作成し、これらのベースラインからの逸脱についてアラートを出します
Answer: C (メーッセージを残す**)**
説明/参照：
Explanation:
パターンマッチングおよび異常検出分析アクティビティは、パケットでは機能しません。
不正解：
A：異常検出は、通常のアクティビティに関するデータを収集します。これによりデータが生成されます。
B：IDSに一致するパターンは、署名データベースを使用して、監視対象のすべてのイベントをその内容に一致させようとします。データベースに存在する既知の攻撃のみを検出できます。
D：異常検出は、通常のアクティビティに関するデータを収集します。通常のアクティビティに関する十分なデータが蓄積されると、異常で発生する可能性のある悪意のあるアクティビティやイベントを検出できます。
参照：
Stewart、James M.、Ed Tittel、およびMike Chapple、CISSP：Certified Information Systems Security Professional Study Guide、第5版、Sybex、インディアナポリス、2011年、p。56

最新問題**: 306**
次のうち、元々は
データ交換にTCP/IPを使用する国防総省？
A. インターネット。
B. イントラネット。
C. エクストラネット。
D. イーサネット。
Answer: A (メーッセージを残す**)**
インターネットは、もともと部門によって資金提供されたWANです。
データ交換にTCP/IPを使用する防御。
出典：KRUTZ、Ronald L.＆VINES、Russel D.、CISSP準備ガイド：マスタリング
コンピュータセキュリティの10のドメイン、2001年、John Wiley＆Sons、99ページ。

最新問題**: 307**
SQLコマンドには、次のうちどれが含まれていませんか？
A. 選択、更新

B. 付与、取り消し
C. 削除、挿入
D. 追加、再リスト
Answer: (解答を表示する**)**
構造クエリ言語（SQL）にはそのようなコマンドはありません。
SQLコマンドには、選択、更新、削除、挿入、付与、置換、復元、および取り消しが含まれます。
一般的なもののほんの一部に名前を付けます。
この質問に使用される参照：
http://technet.microsoft.com/en-us/library/ms186862.aspx
と
KRUTZ、Ronald L.＆VINES、Russel D.、CISSP準備ガイド：の10のドメインをマスターする Computer Security、2001年、John Wiley＆Sons、47ページ。
と
http://www.sqlcommands.net/
と
http://www.cs.utexas.edu/~mitra/csFall2012/cs329/lectures/sql.html

最新問題**: 308**
次のうち、運用管理の重要なセキュリティの側面ではないものはどれですか？
A. ハードウェアの制御。
B. 使用されたデータメディア。
C. リソースを使用するオペレーター。
D. 環境管理。
Answer: D (メーッセージを残す**)**
環境問題に対処することは重要ですが、それらは物理的セキュリティドメインの一部です。
他のすべての回答は、運用セキュリティに直接該当します。

最新問題**: 309**
使用中のデータ制御を実装することの主な利点は次のうちどれですか？
A. データを表示するときは、安全なプロトコルを使用してアクセスする必要があります。
B. データを表示しているときは、許可されたユーザーのみが印刷できます。
C. データが失われた場合、開くには復号化する必要があります。
D. データが失われると、許可されていないユーザーがデータにアクセスできなくなります。
Answer: (解答を表示する**)**

最新問題**: 310**
信頼できるシェルとは何ですか？
A. そのシェルで作業している人は『バストアウト」できず、他のプロセスは『バストイン」できないことを意味します。
B. ユーザーまたはプログラムとカーネル間の通信チャネルであることを意味します。

C. そのシェルで作業している人が、別の信頼できるシェルで他の人と通信できることを意味します。
D. プロセスが他のプロセスのデータを上書きしないことを意味します。
Answer: A (メーッセージを残す**)**
信頼できるシェルとは、そのシェルで作業している人が「バストアウト」できないことを意味します
それ」であり、他のプロセスは「それに突入」することはできません。
この質問を作成するために、次の参照が使用されました。
出典：HARRIS、ション、オールインワンCISSP認定試験ガイド、McGraw-Hill / Osborne、2008年、第5章：セキュリティアーキテクチャと設計（323ページ）。

最新問題**: 311**
次の項目のうち、組織が存続に不可欠な機能を共通に理解するのに最も役立つのはどれですか？
A. リスク評価
B. ビジネス評価
C. 災害復旧計画
D. ビジネスへの影響分析
Answer: D (メーッセージを残す**)**
説明/参照：
Explanation:
BIA（ビジネス影響分析）は機能分析と見なされ、チームはインタビューやドキュメンタリーソースを通じてデータを収集します。ビジネス機能、活動、およびトランザクションを文書化します。ビジネス機能の階層を開発します。最後に、分類スキームを適用して、個々の機能の重要度レベルを示します。
不正解：
A：リスク評価には、潜在的なリスクの特定とリスクの潜在的な影響の評価が含まれます。リスク評価は、重要なビジネス機能の機能分析です。
B：ビジネス評価は、重要なビジネス機能の機能分析です。ビジネスアセスメントは、組織の継続的な存続に不可欠なリソースと、それらのリソースにもたらされる脅威を特定する分析です。
C：災害復旧計画は、災害後にさまざまなITメカニズムを復旧する方法に焦点を当てています。
ディザスタリカバリ計画は、重要なビジネス機能の機能分析です。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、2013、p。905

最新問題**: 312**
被覆通信路分析は、TCSEC評価のどのレベルで最初に導入されましたか？
A. C2以上。
B. B1以上。
C. B2以上。

D. B3以上。
Answer: C (メーッセージを残す)
Orange Bookは、最初にレベルでの被覆通信路分析の要件を紹介します
B2およびB2より上のすべてのレベルでもこれが必要になります。
AIOは、プロセスが送信できるようにする通信パスとして被覆通信路を定義します
システムのセキュリティポリシーに違反する方法で情報を提供します。それは通信チャネルです
2つの連携するプロセスが、システムの情報に違反するような方法で情報を転送できるようにします。
セキュリティポリシー。保護メカニズムが導入されていても、許可されていない情報が
通常は考慮されないエンティティまたはオブジェクトを介してシグナリングメカニズムを使用して転送できます
通信できるようになると、秘密チャネルが存在する可能性があります。
次の答えは正しくありません。
C2以上。オレンジの本は被覆通信路分析のみを必要とするため、正しくありません
レベルB2以上から開始すると、レベルC2はB2より低く、被覆通信路は必要ありません。
分析。
B1以上。オレンジの本は、でのみ被覆通信路分析を必要とするため、正しくありません
レベルB2以上では、レベルB1はB2より低く、被覆通信路分析は必要ありません。
B3以上。オレンジの本は最初に被覆通信路分析を必要とするため、正しくありません。
レベルB2。
この質問に使用される参照：
Hernandez CISSP、Steven（2012-12-21）。CISSP CBK、第3版の公式（ISC）2ガイド
（ISC）2 Press）Kindle Locations 13347-13350）。AuerbachPublications。キンドル版。
と
NIST http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt

最新問題: **313**
ネットワークベースのIDシステムの問題は、ログインしている侵入者によるホストに対する攻撃を検出しないことです。次のうちどれですか。
A. クライアントの端末
B. ゲストのターミナル
C. ホストの端末
D. サーバーの端末
Answer: C (メーッセージを残す)

最新問題: **314**
次のうち、監査証跡の使用ではないものはどれですか？
A. パスワードやインフラストラクチャ構成などの情報を収集します
B. セキュリティ担当者がトランザクションの履歴を追跡できるようにします
C. データの追加、削除、または変更に関する情報を提供します

D. ユーザーの異常な行動パターンの認識を支援することで監視機能を支援します
Answer: A (メーッセージを残す**)**
正解は〝パスワードやインフラストラクチャの構成などの情報を収集する」です。ユーザーのパスワードを収集するために監査を使用しないでください。ただし、他の3つの例で使用されます。

最新問題**: 315**
Orange Bookが基づいているコンピュータセキュリティポリシーモデルは、次のうちどれですか？
A. ベルラパドゥラ
B. データ暗号化標準
C. Kerberos
D. テンペスト
Answer: A (メーッセージを残す**)**
アンダーソンレポートの公開に続いて、セキュリティポリシー要件の正式なモデルと、それらのポリシーモデルをセキュリティカーネルとして実装および実施するメカニズムについて、かなりの調査が開始されました。これらの取り組みの中で際立っていたのは、ESDが後援するベルラパドゥラモデルの開発でした。これは、国防総省のセキュリティポリシーの抽象的な正式な扱いです。[2] モデルは、数学と集合論を使用して、安全な状態の概念、基本的なアクセスモード、および対象にオブジェクトへの特定のアクセスモードを付与するためのルールを正確に定義します。最後に、定理は、ルールがセキュリティを維持する操作であることを示しているため、ルールのシーケンスを安全な状態のシステムに適用すると、システムも安全な新しい状態になります。
定理。

最新問題**: 316**
以下のどのタスクが通常はBCPタスクと見なされますか
DRPタスクよりも？
A. 復旧手順
B. 生命の安全プロセス
C. プロジェクトの範囲
D. 復元手順
Answer: (解答を表示する**)**
事業継続計画を作成する際の多くのプロセスは
災害復旧計画を作成するプロセスと同様に、いくつか
違いがあります。事業継続計画プロセス
BCPに固有のものには、次のものが含まれます。
プロジェクトのスコーピングと役割の割り当て
ビジネスへの影響と脆弱性の評価の作成
代替処理サイトの選択
一方、独自のディザスタリカバリ/緊急管理プロセス
含めることができます：

代替サイトへの移転手順の実施
テストとトレーニングを計画する
データの回復
損傷した機器の回収
出典 :CISSP Examination Textbooks、Volume One :Theory、byS。
Rao Vallabhaneni、SRVProfessionalPublications初版2000
および情報セキュリティ管理ハンドブック、Micki著
クラウスとハロルド F ·ティプトン、アウアーバック、1999年版。

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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: **317**
セキュリティの専門家が組織のビジネス影響分析を完了しました
（BIA）。事業継続計画/災害復旧計画（BCP / DRP）のベストプラクティスに従って、専門家の次のステップは何でしょうか？
A. 組織の復旧チームのメンバーを選択します。
B. 組織の業務を回復する能力をテストするための計画を作成します。
C. 回復戦略を特定して選択します。
D. 資金調達のために経営陣に調査結果を提示します。
Answer: C (メーッセージを残す**)**

最新問題: **318**
災害によって引き起こされた停止コストの決定は、
A. 冗長システムとバックアップのコスト。
B. 停止から回復するためのコスト。
C. 停止による全体的な長期的影響。
D. 停止中に収益が失われました。
Answer: C (メーッセージを残す**)**
セクション :ソフトウェア開発のセキュリティ

最新問題: **319**
以下にリストされているバックアップ方法のうち、おそらくバックアップが必要になるのはどれですか
オペレーターは、システム全体で最も多くのテープを使用します

復元、5日間のローテーションで毎晩異なるテープが使用された場合はどうなりますか？
A. 増分バックアップ方式
B. アドホックバックアップ方式
C. 完全バックアップ方式
D. 差分バックアップ方式
Answer: (解答を表示する**)**
ほとんどのバックアップ方法では、アーカイブファイル属性を使用して決定します
ファイルをバックアップする必要があるかどうか。バックアップソフトウェア
確認することにより、バックアップする必要のあるファイルを決定します
アーカイブファイル属性が設定されている場合、バックアップ手順の後でアーカイブビット値をnullにリセットします。増分バックアップ
メソッドは、それ以降に作成または変更されたファイルのみをバックアップします
アーカイブファイル属性がリセットされたため、最後のバックアップが作成されました。
これにより、バックアップオペレータが実行するために複数のテープが必要になる可能性があります。
完全な復元、ファイルが変更されたすべてのテープ、および
最後の完全バックアップテープを復元する必要があります。
*完全または完全バックアップは、すべてのディレクトリ内のすべてのファイルをバックアップします
最後のバックアップがいつであったかに関係なく、サーバーに保存されます
作成され、ファイルがすでにバックアップされているかどうか。The
アーカイブファイル属性が変更され、ファイルが
バックアップされ、テープまたはテープにはすべてのデータとアプリケーションが含まれます
その上に。ただし、この質問に対する回答は正しくありません。
想定される回答差分バックアップ方式と増分バックアップ方式では、さらに差分テープまたは増分テープが必要になります。
*差分バックアップ方式は、次のようなファイルのみをバックアップします
最後のバックアップが作成されてから作成または変更された
増分バックアップ。ただし、インクリメンタルの違い
バックアップと差分バックアップでは、差分バックアップの完了後にアーカイブファイル属性がリセットされないため、差分バックアップが実行されるたびに変更されたファイルがバックアップされます。これらのファイルは、後続の各差分バックアップ中に次の完全バックアップが発生するまでバックアップされ続けるため、バックアップセットのサイズは次の完全バックアップまで大きくなります。このバックアップ方法の利点は、
バックアップオペレータは、システムを復元するために完全バックアップと1つの差分バックアップのみを必要とします。
表に、これら3つのバックアップ方法を示します。
示す：

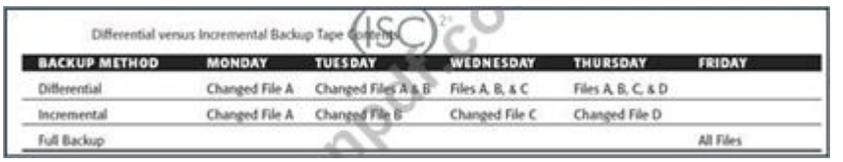


image008
回答 「アドホックバックアップ方法」は気を散らすものです。

最新問題: **320**
オペレーティングシステムが、オブジェクト/メモリ領域を更新せずに、メモリなどの共有リソースを複数のユーザー/アプリケーションまたはサブジェクトが順番に使用することを許可している場合、どのようなセキュリティ問題が存在する可能性が最も高いですか？
A. 残余データの開示。
B. 特権実行状態の不正取得。
C. 被覆通信路を介したデータ漏洩。
D. 致命的な抱擁によるサービス拒否。
Answer: (解答を表示する**)**
を更新せずに、複数のユーザーがオブジェクトを順番に使用できるようにする
オブジェクトは、残余データの開示につながる可能性があります。を排除するための措置を講じることが重要です
残余データの開示のチャンス。
オブジェクトの再利用とは、システムリソースをユーザーに割り当てたり、再割り当てしたりすることです。
適切に、アプリケーションまたはプロセスに。コンピュータシステム上のアプリケーションとサービスは
プログラム機能を実行するために、メモリおよびストレージにオブジェクトを作成または使用します。いくつかの
場合によっては、これらのリソースをさまざまなシステムアプリケーション間で共有する必要があります。でも、
一部のオブジェクトは、アプリケーションに代わって特権タスクを実行するために使用される場合があります。
許可されたユーザーまたはアップストリームアプリケーション。オブジェクトの使用が制御されていない場合、またはそれらのデータ
オブジェクトは使用後に消去されず、許可されていないユーザーまたはプロセスが使用できるようになる可能性があります。
残余データの開示と特権実行状態の不正取得はどちらも
共有メモリとリソースの問題。ヒープ/スタックをクリアしないと、残りが発生する可能性があります
データであり、セキュリティトークン/識別が
そのスペースで維持されます。ただし、これは一般的に、偶発的なものよりも悪意があり、意図的なものです。

最も一般的な問題は、残余データの開示です。
次の答えは正しくありません。
特権実行状態の不正な取得。これは問題ではないため、正しくありません
オブジェクトの再利用を使用します。
秘密チャネルを介したデータ漏洩。最良の答えではないため、正しくありません。秘密チャネルは通信パスです。データの漏洩は、オブジェクトの再利用によって発生する問題ではありません。コンピュータセキュリティでは、秘密チャネルは、コンピュータセキュリティポリシーによって通信が許可されていないプロセス間で情報オブジェクトを転送する機能を作成するコンピュータセキュリティ攻撃の一種です。1973年にLampsonによって作成されたこの用語は、 サービスプログラムのシステム負荷への影響など、情報転送をまったく目的としない チャネル）」と定義されています。COMPUSECによるアクセス制御の対象となる正当なチャネルと区別するため。致命的な抱擁によるサービス拒否。それはただの批判者であるため、正しくありません。
参照 :Hernandez CISSP、Steven 2012-12-21）。CISSP CBKの公式 ISC）2ガイド、第3版（ISC）2 Press）Kindleの場所4174-4179）。AuerbachPublications。キンドル版。および
https://www.fas.org/irp/nsa/rainbow/tg018.htmおよびhttp://en.wikipedia.org/wiki/Covert_channel

最新問題: **321**
電子記憶媒体を修理のために第三者に返却する場合の効果的な方法は何ですか？
A. メディアの安全な取り扱いに関して第三者と契約を結ぶ。
B. メディアに組織の名前を示すラベルが付けられていないことを確認します。
C. 機密データを含む可能性のあるメディアの物理的に破損した部分。
D. メディアを分解し、機密データを含む可能性のある部品を削除します。
Answer: A (メーッセージを残す**)**

最新問題: **322**
次の戦略のうち、悪意のある内部関係者が機密情報を漏洩するリスクに最も包括的に対処するのはどれですか？
A. データ損失保護 DIP）、ファイアウォール、データ分類
B. 身元調査、データ暗号化、Webプロキシ
C. スタッフの審査、最小特権アクセス、データ損失保護 DLP）
D. 最小特権アクセス、データ損失保護 DLP）、物理アクセス制御
Answer: D (メーッセージを残す**)**

最新問題: **323**
強制アクセス制御では、オブジェクトにアクセスするためのサブジェクトの許可は、以下に依存します。
A. 役割。
B. ラベル。
C. タスク。

D. アイデンティティ。
Answer: B (メーッセージを残す**)**
正解はラベルです。強制アクセス制御は、ラベルを使用して
に応じて、被験者がオブジェクトにアクセスできるかどうかを判断します
被験者のクリアランス。回答の役割は非裁量で適用されます
タスクと同様にアクセス制御。アイデンティティは、裁量で使用されます
アクセス制御。

最新問題**: 324**
必要なときに必要な場所でデータにアクセスできることを確認するのは、次のうちどれですか。
A. 守秘義務
B. 整合性
C. 受容性
D. 可用性
Answer: (解答を表示する**)**
これは、ネットワークセキュリティの柱の1つです。必要なときにアクセスできれば、データは利用可能であると言えます。これは質問で言及されていることです。可用性とは、必要なときに必要な場所でデータにアクセスすることを指します。
機密性は、第三者の傍受に対する暗号化とデータ保護を扱います。整合性はデジタル署名を処理し、データが変更されていないことを保証します。受容性は関連用語ではありません。

最新問題**: 325**
秘密のストレージと秘密のタイミングチャネルの両方から保護する必要があるレベルはどれですか？
A. B3およびA1
B. B2、B3、A1
C. A1
D. B1、B2、B3、A1
Answer: A (メーッセージを残す**)**
参照 :302ページKrutz :CISSP準備ガイド :ゴールドエディション

最新問題**: 326**
暗号化は、次の選択肢のどれに関係しませんか？
A. 可用性
B. 整合性
C. 守秘義務
D. 検証
Answer: (解答を表示する**)**

暗号化ドメインは、情報の整合性、機密性、および信頼性を確保するために、情報を偽装する原則、手段、および方法に対応しています。他のドメインとは異なり、暗号化は可用性の標準を完全にはサポートしていません。
可用性
暗号化は、情報セキュリティの3つのコア原則すべてをサポートします。多くのアクセス制御システムは、暗号化を使用して、パスワードを使用してシステムへのアクセスを制限しています。多くのトークンベースの認証システムは、暗号化ベースのハッシュアルゴリズムを使用してワンタイムパスワードを計算します。不正アクセスを拒否すると、攻撃者がシステムやネットワークに侵入して損害を与えることを防ぎ、許可されたユーザーがデータを損傷または破壊した場合にアクセスを拒否します。
機密性暗号化は、メッセージを変更または非表示にすることで機密性を提供します。これにより、理想的には、意図した受信者以外の誰もがメッセージを理解できないようになります。
整合性暗号化ツールは、受信者がメッセージが変更されていないことを確認できる整合性チェックを提供します。暗号化ツールは、メッセージの変更を防ぐことはできませんが、メッセージの意図的または偶発的な変更を検出するのに効果的です。
暗号化システムの追加機能上記の情報セキュリティの3つのコア原則に加えて、暗号化ツールにはさらにいくつかの利点があります。
否認防止
信頼できる環境では、発信元の認証は簡単な方法で提供できます
キーの制御。受信者は、メッセージが暗号化されていることをある程度保証しています。
送信者、および送信者は、メッセージが受信された後は変更されていないことを信頼しています。
でも、
より厳格で信頼性の低い環境では、
メッセージを送信した第三者であり、メッセージが実際に右側に配信されたこと
受信者。これは、デジタル署名と公開鍵暗号化を使用して実現されます。The
これらのツールを使用すると、第三者が検証できるレベルの否認防止が提供されます。
メッセージを受信したら、受信者がメッセージを変更できないようにするにはどうすればよいですか
変更されたメッセージが送信者によって送信されたものであることに異議を唱えますか？否認防止
配信により、受信者がメッセージを変更したり、メッセージが
元の状態で。これは、公開鍵暗号と
デジタル署名であり、信頼できるサードパーティによって検証可能です。
認証
認証とは、誰かまたは何かがそれが宣言したものであるかどうかを判断する機能です。これは
キーにアクセスできる人だけができるので、主にキーの制御を介して行われます
メッセージを暗号化します。これは、レビューされる原産地の否認防止ほど強力ではありません。
間もなく暗号化関数はいくつかの方法を使用して、メッセージが送信されていないことを確認します

変更または変更されました。これらには、ハッシュ関数、デジタル署名、およびメッセージ認証が含まれます
コード（MAC）。主な概念は、受信者が変更を検出できることです。
偶然であろうと故意であろうと、メッセージに対してなされた。
アクセス制御
暗号化ツールを使用することで、ログインからのアクセス制御の多くの形式がサポートされます
機密ファイルやメッセージへのアクセスを防ぐためのパスワードとパスフレーズを介して。の
すべての場合において、アクセスは正しいアクセス権を持っていた個人に対してのみ可能です。
暗号化キー。
CLEMENTからのメモ：
あなたが見てきたように、この質問はごく最近、公式の最新のコンテンツで更新されました
CISSP CBKバージョン3のISC2ガイド（OIG）。
私自身、暗号化は可用性の面では役に立たないということに同意します。
たとえば、キーを紛失した場合でも、逆の場合があります。そのような場合、あなたは失うでしょう
データへのアクセスと可用性に悪影響を及ぼします。しかし、ISC2は、私が何を考えているのか、何を考えているのかについてではありません。
あなたが思うに、彼らは彼らが主張し、明確に述べている世界観を持っています
暗号化は、完全に対処していなくても、可用性に対処します。
彼らは、暗号を今日の包括的なツールと見なしています。使用できる場所
たとえば、次の方法でデータの破損を回避するのに役立つ認証目的
許可されていないユーザーによる違法なアクセス。
質問は目的のためにこのように表現されています、それはCISSP試験のコンテキストに非常に固有です
ISC2は、暗号化が完全に対応していないと述べている場合でも、暗号化が可用性に対応していると説いています
それ。これは彼らの本の最後の版で新しいものであり、あなたが知っておくべきことです。
よろしくお願いします
クレメント
次の用語は、ソフトウェア開発セキュリティドメインからのものです。
検証：製品、サービス、またはシステムが顧客のニーズを満たしていることの保証
他の特定された利害関係者。多くの場合、外部顧客の受け入れと適合性が関係します。
以下の検証と比較してください。」
検証：製品、サービス、またはシステムが以下に準拠しているかどうかの評価
規制、要件、仕様、または課せられた条件。多くの場合、これは内部プロセスです。
検証と対比してください。」
上記の用語は、ソフトウェア開発セキュリティドメインからのものです。
この質問に使用される参照：
シュナイター、アンドリュー（2013-04-15）。CISSP CBK、第3版の公式（ISC）2ガイド：

暗号化（Kindleの場所227-244）。。キンドル版。
と
シュナイター、アンドリュー（2013-04-15）。CISSP CBK、第3版の公式（ISC）2ガイド：
暗号化（Kindleの場所206-227）。。キンドル版。
と
http://en.wikipedia.org/wiki/Verification_and_validation

最新問題: **327**
攻撃の種類は次のように説明されます。攻撃者はブロードキャストアドレスのリストを配列に格納し、それらのアドレスのそれぞれにスプーフィングされたicmpエコー要求を連続して送信して再開します。攻撃者がパケットの送信元として使用するスプーフィングされたIPアドレスは、ターゲット/被害者のIPアドレスです。
A. スマーフ攻撃
B. フラグルアタック
C. ランドアタック
D. リプレイアタック
Answer: A (メーッセージを残す**)**
Smurf攻撃は、多数のインターネットが攻撃するサービス拒否攻撃です。
意図された被害者のスプーフィングされた送信元IPを持つ制御メッセージプロトコル（ICMP）パケットは
IPブロードキャストアドレスを使用してコンピュータネットワークにブロードキャストします。ネットワーク上のほとんどのデバイスは、デフォルト設定で、に応答を送信することでこれに応答します。
送信元IPアドレス。これらを受信して応答するネットワーク上のマシンの数
パケットが非常に大きいため、被害者のコンピュータはトラフィックで溢れています。これにより、速度が低下する可能性があります
被害者のコンピュータが作業できなくなるまで。
Smurfという名前は、攻撃プログラムのソースコードであるファイル「smurf.c」に由来しています。
1997年にTFreakからリリースされました。
著者は、攻撃を次のように説明しています。
「スマーフ」攻撃は非常に単純です。配列に格納するブロードキャストアドレスのリストがあり、そして、スプーフィングされたicmpエコー要求をこれらのアドレスのそれぞれに直列に送信し、再開します。その結果、スプーフィングされたIPに対する攻撃が発生し、使用されるブロードキャストアドレスの量に応じて、多くのコンピュータがエコー要求に応答します。
緩和：
-この脅威を軽減するための最良の方法は、物理ネットワークインフラストラクチャへのアクセスを制御することです。もしも
攻撃者は攻撃を送信できません。この攻撃は明らかに機能しません。

-現在、ネットワークへのアクセスを制御するための推奨される方法は、802.1Xを使用することです-
証明書のセキュリティ。
-また、最近のオペレーティングシステムでは、通常、ブロードキャストアドレスへのPINGは許可されておらず、
試行するとエラーメッセージを返します。
次の答えは正しくありません。
-フラグルアタック：閉じるが、完全には正しくない。Fraggle攻撃は、SmurfAttackが使用するICMPではなくUDPを使用します。
-ランドアタック：申し訳ありませんが、正しくありません。LAND攻撃は、送信元と宛先のIPアドレスが被害者と同じであるターゲットに送信される一連のパケットです。
-リプレイアタック :これはシステムの脆弱性を利用する攻撃ではないため、正解ではありません。
この質問を作成するために、次の参照が使用されました :http://en.wikipedia.org/wiki/Smurf_attackおよびhttp://searchsecurity.techtarget.com/answer/What-is-a-land-attackおよびhttp
://www.phreak.org/archives/exploits/denial/smurf.c

最新問題: **328**
データベース内のデータの正規化には、次のうちどれを除いてすべてまたは一部を含めることができますか？
A. 同じテーブルから重複する列を削除します。
B. キー全体に依存するフィールドとは別のテーブルにフィールドを配置することにより、部分的なキーへの機能依存性を排除します
C. 非キーフィールドを別のテーブルに配置することにより、非キーフィールドへの機能依存性を排除しました。このレベルでは、すべての非キーフィールドは主キーに依存しています。
D. 別々のテーブルに配置することにより、重複するキーフィールドを排除します。
Answer: D (メーッセージを残す**)**
1.同じテーブルから重複する列を削除します。
2。キー全体に依存するフィールドとは別のテーブルにフィールドを配置することにより、部分的なキーへの機能依存性を排除します。
3。非キーフィールドを別のテーブルに配置することにより、非キーフィールドへの機能依存性を排除しました。このレベルでは、すべての非キーフィールドは主キーに依存しています。
データベースを作成する場合、正規化とは、データベースを使用した結果が常に明確で意図したとおりになるように、データベースをテーブルに編成するプロセスです。
正規化は、データベース内でデータを複製する効果があり、多くの場合、追加のテーブルが作成されます。（正規化はデータの重複を増やす傾向がありますが、冗長性は導入されません。これは不要な重複です。）正規化は通常、データベースに存在する必要のあるデータオブジェクトを識別し、それらの関係を識別し、必要なテーブルと各テーブル内の列を定義します。
データの正規化の簡単な例は、次の表で構成されている場合があります。
購入した顧客アイテム購入価格

トーマスシャツ$40
マリアテニスシューズ$35
Evelynシャツ$40
パジャロパンツ$25
このテーブルがアイテムの価格を追跡する目的で使用され、顧客の1人を削除する場合は、価格も削除します。データを正規化するということは、これを理解し、このテーブルを2つのテーブルに分割して問題を解決することを意味します。1つは各顧客と購入した製品に関する情報、もう1つは各製品とその価格に関する情報です。どちらかのテーブルに追加または削除しても、もう一方には影響しません。
リレーショナルデータベーステーブルの正規化度が定義されており、次のものが含まれます。
第一正規形（1NF）。これは正規化の「基本的な」レベルであり、通常、データベースの定義に対応します。
行と列のある2次元テーブルが含まれています。
各列は、テーブル全体で表されるサブオブジェクトまたはオブジェクトの属性に対応します。
各行は、そのサブオブジェクトまたは属性の一意のインスタンスを表し、他の行とは何らかの方法で異なっている必要があります（つまり、重複する行はできません）。
任意の列のすべてのエントリは同じ種類である必要があります。たとえば、ラベルの付いた列で「顧客」、顧客の名前または番号のみが許可されます。
すべてのテーブルが繰り返しグループのない2次元である場合、エンティティは第一正規形（1NF）になります。
基になるすべてのドメインにアトミック値のみが含まれている場合、行は第一正規形（1NF）になります。1NFは、グループを別々のテーブルに配置し、それらを1対多の関係で接続することにより、グループの繰り返しを排除します。関連する属性のセットごとに個別のテーブルを作成し、主キーを使用して各レコードを一意に識別します。
同じテーブルから重複する列を削除します。
関連データのグループごとに個別のテーブルを作成し、一意の列または列のセット（主キー）で各行を識別します。
2番目の正規形（2NF）。このレベルの正規化では、別の列の内容を決定するものではないテーブル内の各列は、それ自体がテーブル内の他の列の関数である必要があります。たとえば、顧客ID、販売された製品、および販売されたときの製品の価格を含む3つの列を持つテーブルでは、価格は顧客ID（割引の対象）と特定の製品の関数になります。
エンティティは、Firstであるという要件を満たす場合、Second Normal Form（2NF）になります。
正規形（1NF）および追加：
複合主キーはありません。これは、主キーを個別の論理エンティティに分割できないことを意味します。
すべての非キー列は、主キー全体に機能的に依存しています。
行が第1正規形であり、すべての非キー属性が完全にキーに依存している場合に限り、行は第2正規形になります。

2NFは、キー全体に依存するフィールドとは別のテーブルにフィールドを配置することにより、部分的なキーへの機能依存性を排除します。例は、交差するエンティティを使用して多くの：多くの関係を解決することです
3番目の正規形（3NF）。2番目の正規形では、テーブルの1つの行を変更すると、別のテーブルからこの情報を参照するデータに影響を与える可能性があるため、変更は引き続き可能です。たとえば、先ほど引用した顧客テーブルを使用して、顧客の購入を説明する行を削除すると（おそらく返品のため）、製品に特定の価格があるという事実も削除されます。3番目の正規形では、これらのテーブルは2つのテーブルに分割され、製品の価格が個別に追跡されます。
エンティティは、第2正規形であるという要件を満たす場合、第3正規形（3NF）になります。
通常の形式（2NF）および追加：
非キーフィールドへの機能依存性は、それらを別のテーブルに配置することで排除されます。このレベルでは、すべての非キーフィールドは主キーに依存しています。
行が第2正規形であり、主キーの説明に寄与しない属性が別のテーブルに移動された場合にのみ、行は第3正規形になります。例として、ルックアップテーブルの作成があります。
ドメイン/キーの正規形（DKNF）。キーは、テーブルの各行を一意に識別します。ドメインは、属性の許容値のセットです。キーとドメインの制限を適用することにより、データベースは変更の異常から解放されます。DKNFは、ほとんどの設計者が達成しようとしている正規化レベルです。
参照：
KRUTZ、Ronald L.＆VINES、Russel D.、CISSP準備ガイド：10をマスターする
Domains of Computer Security、2001年、John Wiley＆Sons、47ページ。
と
http://psoug.org/reference/normalization.html
と
Tech Target SearcSQLServer：
http://searchsqlserver.techtarget.com/definition/normalization?vgnextfmt=print

最新問題: **329**
通信チャネルが任意の数の可変ビットレートデジタルチャネルまたはデータストリームに分割されるデータを多重化する方法は、次のうちどれですか。この方法では、送信する情報を持つ物理チャネルに帯域幅を動的に割り当てますか？
A. 時分割多重
B. 非同期時分割多重
C. 統計多重化
D. 周波数分割多重
Answer: C (メーッセージを残す**)**
統計多重化は、動的帯域幅割り当て（DBA）と非常によく似た、通信リンク共有の一種です。統計多重化では、通信チャネルは任意の数の可変ビットレートデジタルチャネルまたはデータストリームに分割されます。リンク共有は、各チャネルを介して転送されるデータストリームの瞬間的なトラフィック需要に適合します。これは、一般的な時分割多重（TDM）や周波数分割多重など、リンクの固定共有を作成する代わりの方法です。

FDM）。正しく実行されると、統計多重化は、統計多重化ゲインと呼ばれるリンク使用率の向上をもたらします。
一般に、データを多重化する方法には次のものがあります。
時分割多重（TDM）：各データチャネルからの情報には、送信するデータがあるかどうかに関係なく、事前に割り当てられたタイムスロットに基づいて帯域幅が割り当てられます。時分割多重化は主にデジタル信号に使用されますが、2つ以上の信号またはビットストリームが転送され、1つの通信チャネルにサブチャネルとして同時に表示されるが、チャネルを物理的に交代させるアナログ多重化に適用できます。時間領域は、サブチャネルごとに1つずつ、固定長の複数の繰り返しタイムスロットに分割されます。サブチャネル1のサンプルバイトまたはデータブロックは、タイムスロット1、サブチャネル2、タイムスロット2などで送信されます。1つのTDMフレームは、サブチャネルごとに1つのタイムスロットと同期チャネル、場合によってはエラー修正チャネルで構成されます。同期前。
非同期時分割多重（ATDM）データチャネルからの情報には、動的に割り当てられたタイムスロットを介して、必要に応じて帯域幅が割り当てられます。ATMは、回線交換ネットワークとパケット交換ネットワークの両方に類似した機能を提供します。ATMは、非同期時分割多重化を使用し、データをセルと呼ばれる小さな固定サイズのパケット（ISO-OSIフレーム）にエンコードします。これは、インターネットなどのアプローチとは異なります
可変サイズのパケットとフレームを使用するプロトコルまたはイーサネット。ATMは、実際のデータ交換を開始する前に2つのエンドポイント間に仮想回線を確立する必要があるコネクション型モデルを使用します。これらの仮想回線は、「永続的」、つまり通常はサービスプロバイダーによって事前構成されている専用接続、または「切り替え」、つまりシグナリングを使用して通話ごとに設定され、通話が終了すると切断される場合があります。
周波数分割多重（FDM）：各データチャネルからの情報には、トラフィックの信号周波数に基づいて帯域幅が割り当てられます。電気通信では、周波数分割多重（FDM）は、通信媒体で利用可能な全帯域幅を一連の重複しない周波数サブバンドに分割する手法であり、各サブバンドは個別の信号を伝送するために使用されます。これにより、無線スペクトル、ケーブル、光ファイバーなどの単一の伝送媒体を多くの信号で共有できます。
この質問に使用される参照：
http://en.wikipedia.org/wiki/Statistical_multiplexing
と
http://en.wikipedia.org/wiki/Frequency_division_multiplexing
と
Information Systems Audit and Control Association、Certified Information Systems Auditor 2002レビューマニュアル、第3章：技術インフラストラクチャと運用慣行（114ページ）。

最新問題: **330**
次のうち、トランザクション冗長性の実装はどれですか？
A. オンサイトミラーリング
B. 電子ボールティング

C. リモートジャーナリング
D. データベースシャドウイング
Answer: A (メーッセージを残す**)**
説明/参照：
Explanation:
オンサイトミラーリングは、トランザクションの冗長性ソリューションです。
不正解：
B：電子ボールトはトランザクション冗長性ソリューションの一種です。電子ボールトは、変更されたファイルのコピーを作成し、定期的にオフサイトのバックアップサイトに送信します。
C :リモートジャーナリングは、トランザクション冗長性ソリューションの一種です。リモートジャーナリングは、データをオフサイトに送信する方法です。これには通常、ジャーナルまたはトランザクションログのオフサイト機能への移動のみが含まれ、実際のファイルは含まれません。これらのログには、個々のファイルに対して行われたデルタ（変更が含まれています。データが破損していて復元が必要な場合、銀行はこれらのログを取得できます。これらのログは、失われたデータを再構築するために使用されます。
D :データベースシャドウイングは、トランザクション冗長性ソリューションの一種です。これはデータベースで使用されるミラーリングテクノロジであり、冗長性を確保するために情報が少なくとも2台のハードドライブに書き込まれます。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、2013、pp.938-939

最新問題**: 331**
TCPラッパーの制限は何ですか？
A. 実行中のUDPサービスへのアクセスを制御できません。
B. パケットがアプリケーション層に到達する前にパケットを停止するため、一部のプロキシサーバーが混乱します。
C. hosts。*アクセス制御システムには、複雑なディレクトリツリーが必要です。
D. 高すぎる。
Answer: (解答を表示する**)**
説明/参照：
Explanation:
TCP Wrappersを使用すると、TCPサービスへのアクセスを制限できますが、UDPサービスへのアクセスは制限できません。
TCPラッパーは、ユーザーIDまたはシステムIDに基づいてポートとリソースへのアクセスを制限することにより、基本的なファイアウォールとして機能できるアプリケーションです。TCPラッパーの使用は、ポートベースのアクセス制御の一形態です。
不正解：
B :TCPラッパーの問題は、プロキシサーバーを混乱させることではありません。問題は、UDPトラフィックをフィルタリングしないことです。

C :hosts。*アクセス制御システムは、複雑なディレクトリツリーを必要としません。最も単純な構成では、デーモン接続ポリシーは、ファイル内のオプションに応じて、許可またはブロックのいずれかに設定されます
/etc/hosts.allow。FreeBSDのデフォルト設定は、inetdで始まるデーモンへのすべての接続を許可することです。
D :UNIX / Linuxシステムでは、TCPラッパーはディストリビューションに含まれており、無料で提供されます。
参照：
Stewart、James M.、Ed Tittel、およびMike Chapple、CISSP :Certified Information Systems Security Professional Study Guide、第5版、Sybex、インディアナポリス、2011年、p。118

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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: **332**
物理的セキュリティドメインは、企業のリソースと機密情報を物理的に保護するための基礎となる3つの領域に焦点を当てています。次のうち、これらの領域の1つではないものはどれですか？
A. 脅威
B. 対策
C. 脆弱性
D. リスク
Answer: B (メーッセージを残す**)**
対策は、リスク、脅威、および脆弱性を軽減するために使用され、保護される領域ではありません。セキュリティは組織とそのインフラストラクチャにとって非常に重要であり、物理的セキュリティも例外ではありません。物理的セキュリティには、これまでに対処されてきた他の種類のセキュリティとは異なる一連の脅威、脆弱性、およびリスクが含まれます。
物理的セキュリティメカニズムには、サイトの設計とレイアウト、環境コンポーネント、緊急時対応の準備、トレーニング、アクセス制御、侵入検知、および電源と防火が含まれます。物理的セキュリティメカニズムは、人、データ、機器、システム、施設、および企業資産の長いリストを保護します。

最新問題: **333**
Bell-LaPadulaセキュリティモデルの主な焦点は何ですか？
A. 説明責任
B. 整合性

C. 守秘義務
D. 可用性
Answer: C (メーッセージを残す**)**
Bell-LaPadulaモデルは、機密性を扱う正式なモデルです。
Bell-LaPadulaモデル（略称BLP）は、アクセスを強制するために使用されるステートマシンモデルです。
政府および軍のアプリケーションでの制御。デビッドエリオットベルとレナードによって開発されました
J.LaPadula、米国国防総省（DoD）のマルチレベルセキュリティ（MLS）ポリシーを正式化するためのRogerR.Schellからの強力なガイダンスに続きます。このモデルは、コンピューターセキュリティポリシーの正式な状態遷移モデルであり、オブジェクトのセキュリティラベルとサブジェクトのクリアランスを使用する一連のアクセス制御ルールを記述します。セキュリティラベルは、最も機密性の高いもの（「トップシークレット」など）から最も機密性の低いもの（「未分類」や「公開」など）までさまざまです。
Bell-LaPadulaモデルは、データの整合性を保護するためのルールを説明するBiba Integrityモデルとは対照的に、データの機密性と機密情報へのアクセスの制御に重点を置いています。この正式なモデルでは、情報システムのエンティティはサブジェクトとオブジェクトに分割されます。
「安全な状態」の概念が定義されており、各状態遷移が保持されることが証明されています
安全な状態から安全な状態に移行することによるセキュリティ、それによってシステムが誘導的に証明する
モデルのセキュリティ目標を満たします。Bell-LaPadulaモデルは、
コンピュータネットワークシステムで許容される状態のセットを備えたステートマシン。からの移行
ある状態から別の状態への遷移関数によって定義されます。
オブジェクトへのサブジェクトの唯一の許可されたアクセスモードの場合、システム状態は「安全」であると定義されます
セキュリティポリシーに準拠しています。特定のアクセスモードが許可されているかどうかを判断するには、
対象のクリアランスは、オブジェクトの分類と比較されます（より正確には、
分類とコンパートメントのセットの組み合わせ、セキュリティレベルを構成する）かどうかを判断する
サブジェクトは特定のアクセスモードに対して許可されています。
クリアランス/分類スキームは、格子で表されます。モデルは2つを定義します
強制アクセス制御（MAC）ルールと3つの任意アクセス制御（DAC）ルール
セキュリティプロパティ：
単純なセキュリティプロパティ特定のセキュリティレベルのサブジェクトは、
より高いセキュリティレベル（読み取りなし）。
-property（「Star」-propertyと読みます）-特定のセキュリティレベルのサブジェクトは、

より低いセキュリティレベルのオブジェクト（評価減なし）。-プロパティは、閉じ込めとも呼ばれます
財産。
随意セキュリティプロパティ随意アクセスを指定するためのアクセスマトリックスの使用
コントロール。
以下は不正解です。
説明責任は正しくありません。説明責任では、アクションがユーザーに追跡可能である必要があります。
それらを実行し、ベルラパドゥラモデルでは対処されていません。
整合性が正しくありません。整合性は、ベルラパドゥラではなくビバモデルで扱われます。
可用性が正しくありません。可用性は、データ/サービスが利用可能であることを保証することに関係しています。
サービスレベル目標で指定され、ベルラパドゥラによって対処されていない許可されたユーザーモデル。
参照：
CBK、pp.325-326
AIO3、279～284ページ
AIOv4セキュリティのアーキテクチャと設計（333～336ページ）
AIOv5セキュリティアーキテクチャと設計（336～338ページ）
ウィキペディア（https://en.wikipedia.org/wiki/Bell-La_Padula_model）

最新問題: **334**
ルールベースのアクセス制御（RuBAC）アクセスは、ルールによって決定されます。このようなルールは、アクセス制御のどのカテゴリに当てはまりますか？
A. 随意アクセス制御（DAC）
B. 強制アクセス制御（MAC）
C. 非随意アクセス制御（NDAC）
D. 格子ベースのアクセス制御
Answer: C (メーッセージを残す**)**
説明/参照：
Explanation:
ルールベースのアクセス制御は、ユーザーが自分の裁量に基づいてアクセスを決定できないため、裁量的ではないと見なされます。
不正解：
A：随意アクセス制御（DAC）を使用すると、データ所有者は、所有するファイルとリソースにアクセスできるサブジェクトを指定できます。
B：強制アクセス制御は任意ではないと見なされ、セキュリティラベルシステムに基づいています。D：格子ベースのアクセス制御は、ラベルベースのアクセス制御またはルールベースのアクセス制御制限として知られています。
参照：

Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、2013、pp.220-228
https://en.wikipedia.org/wiki/Lattice-based_access_control

最新問題: **335**
多くの組織がソフトウェア開発における語彙の難読化を思いとどまらせているのはなぜですか？
A. 災害後のシステムの復旧に関する問題
B. テストケースの作成に関する問題
C. データ接続の維持に関する問題
D. コードのコンパイルに関する問題
Answer: B (メーッセージを残す**)**

最新問題: **336**
Wi-Fi環境でデータの機密性を最も強力に保護するのは次のうちどれですか？
A. Wi-Fi Protected Access 2（WPA2）+カウンターモードと暗号ブロック連鎖メッセージ認証コードプロトコル（CCMP）
B. Wi-Fi Protected Access（WPA）+ Temporal Key Integrity Protocol（TKIP）
C. Wi-Fi Protected Access 2（WPA2）+ Advanced Encryption Standard（AES）
D. Wired Equivalent Privacy（WEP）+ Advanced Encryption Standard（AES）
Answer: C (メーッセージを残す**)**

最新問題: **337**
統計的異常検出とパターンマッチングの両方の弱点は次のうちどれですか？
A. スケーリングする能力の欠如。
B. 学習モデルの欠如。
C. リアルタイムで実行できない。
D. すべてのイベントを監視するための要件。
Answer: (解答を表示する**)**
知識ベースのIDシステムのデメリット :このシステムはリソースを大量に消費します。ナレッジデータベースは継続的にメンテナンスと更新を必要とします。新しい、固有の、または元の攻撃は見過ごされがちです。動作ベースのIDシステムの欠点 :システムは、誤警報率が高いという特徴があります。ハイポジティブはIDシステムの最も一般的な障害であり、システムを使用できなくするデータノイズを生成する可能性があります。ネットワークシステムにいる間のユーザーのアクティビティと動作は、動作ベースのIDシステムを効果的に実装するのに十分なほど静的ではない可能性があります。-Ronald Krutz CISSP PREPガイド（ゴールドエディション）88ページ

最新問題: **338**
ネットワークのさまざまなコンポーネント（デバイス、プロトコル、アクセス方法など）が連携して機能することを保証する通信製品およびサービスとは、次のことを指します。
A. Netwareアーキテクチャ。
B. ネットワークアーキテクチャ。

C. WANアーキテクチャ。
D. マルチプロトコルアーキテクチャ。
Answer: B (メーッセージを残す**)**
説明/参照：
Explanation:
ネットワークアーキテクチャは、通信ネットワークの設計です。これは、ネットワークの物理コンポーネントとその機能構成および構成、プロトコルとアクセス方法を含むその運用原則と手順、およびその運用で使用されるデータ形式を指定するためのフレームワークです。
不正解：
A :NovellNetwareはベンダーNovellに固有です。
C :WANアーキテクチャは、ネットワークのさまざまなコンポーネントには使用されません。これは、異なるローカルネットワークが他のネットワークと通信できるようにするコンポーネントに使用されます。
D :プロトコルだけでなく、物理コンポーネントも含める必要があります。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、New York、2013、p。246

最新問題**: 339**
ペネトレーションテストに続いて、組織は最初に何をすべきですか？
A. すべてのセキュリティポリシーと手順を確認します。
B. スタッフがセキュリティのトレーニングを受けていることを確認します。
C. 完全なセキュリティ評価を実施する必要があるかどうかを判断します。
D. テスト結果で特定された問題を評価します。
Answer: (解答を表示する**)**

最新問題**: 340**
セキュリティが組織文化全体の一部であることを保証するために組織が実行する最も重要な活動は次のうちどれですか？
A. セキュリティポリシーがすべての従業員に発行されていることを確認します。
B. セキュリティインシデントの正式なレビューを実行します。
C. 上級管理職と協力してビジネス目標を達成します。
D. セキュリティ監査のプログラムを管理します。
Answer: B (メーッセージを残す**)**

最新問題**: 341**
ニューラルネットワークは、さまざまなアルゴリズムを使用して次のことを学習します。
A. ナレッジベースでルールを実行します。
B. データに適用される重みを調整します。
C. 専門家の考えをエミュレートします。
D. 推論エンジンをエミュレートします。

Answer: B (メーッセージを残す)
正解は、ニューラルネットワークがさまざまな方法で学習することです。
データに適用される重みを調整するアルゴリズム。
他の答えはエキスパートシステムで参照される用語です。

最新問題: **342**
アプリケーションレベルのファイアウォールは以下を作成します。
A. ワークステーションクライアントとサーバー間の仮想回線
B. ワークステーションクライアントとサーバー間の実際の回路
C. ワークステーションホストとサーバー間の一時的な回路
D. ワークステーションゲストとサーバー間の架空の回路
Answer: A (メーッセージを残す)

最新問題: **343**
次のうち、トラステッドプラットフォームモジュール（TPM）の一部であるのはどれですか？
A. データと署名キーの両方を安全な方法で保存するための不揮発性の改ざん防止ストレージ
B. デジタルキーの管理とデジタル署名の高速化を目的とした安全なプロセッサ
C. コンピューター機能にアクセスするためのプラットフォームに依存しないソフトウェアインターフェース
D. コンピューティングプラットフォームの状態を「測定」するための方法またはメトリックを指定する、保護されたPre-Basic入出力システム（BIOS）
Answer: A (メーッセージを残す)

最新問題: **344**
TCSECレベルB3およびA1オペレーティングシステムのメモリ管理では、「データの隠蔽」を利用できます。これは何を意味するのでしょうか？
A. システム関数は階層化されており、特定の層の関数はいずれもその層の外部のデータにアクセスできません。
B. 監査プロセスとそのメモリアドレスは、ユーザープロセスからアクセスできません。
C. セキュリティプロセスのみがリングゼロメモリへの書き込みを許可されます。
D. これは強力な暗号化暗号の一種です。
Answer: A (メーッセージを残す)
説明/参照：
Explanation:
データの非表示はデータを保護しているため、これはより高いレベルでのみ利用可能であり、各レイヤーのソフトウェアが独自のグローバルデータを維持し、レイヤー外のデータを直接参照しない場合は、レイヤーによっても実行されます。
不正解：
B：監査プロセスとそのメモリアドレスにユーザープロセスがアクセスできないのは、データの非表示が提供されていないため、正しくありません。

C :セキュリティプロセスのみがリングゼロメモリへの書き込みを許可されています。これは正しくありません。セキュリティカーネルがこれを担当します。
D :これはデータ隠蔽の定義に準拠していないため、強力な暗号化暗号の形式は正しくありません。

最新問題: **345**
理想的な動作湿度範囲は、40%から60%と定義されています。低湿度（40%未満）は、コンピューター部品にどのような種類の問題を引き起こす可能性がありますか？
A. 静電気
B. 電気めっき
C. エネルギーメッキ
D. エレメントメッキ
Answer: A (メーッセージを残す**)**
説明/参照：
Explanation:
データセンター内で適切な温度と湿度のレベルを維持することが重要です。そのため、この部屋専用にHVACシステムを実装する必要があります。温度が高すぎると、コンポーネントが過熱してオフになる可能性があります。温度が低すぎると、コンポーネントの動作が遅くなる可能性があります。湿度が高いと、コンピューター部品の腐食が発生する可能性があります。湿度が低い場合は、静電気が発生する可能性があります。この静電気により、デバイスがショートし、情報が失われる可能性があります。このため、データセンターには、建物の他の部分とは別に、独自の温度と湿度の制御が必要です。
不正解：
B：電気めっきは低湿度によるものではありません。したがって、この答えは正しくありません。
C :エネルギーメッキは低湿度によるものではありません。したがって、この答えは正しくありません。
D :エレメントメッキは低湿度によるものではありません。したがって、この答えは正しくありません。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、2013、p。456

最新問題: **346**
プロトコルエンティティ間の通信の頻度、長さ、および発信元と宛先のパターンのマスキングに関係するのは、次のうちどれですか？
A. マスキング分析
B. プロトコル分析
C. トラフィック分析
D. パターン分析
Answer: C (メーッセージを残す**)**

トレンド分析と呼ばれることもあるトラフィック分析は、データの特性（メッセージの長さ、メッセージの頻度など）と送信パターン（送信される実際の情報の知識ではなく）を分析することを含む、侵入者が採用する手法です。侵入者に役立つ情報を推測します）。-Ronald Krutz CISSP PREPガイド（ゴールドエディション）323ページ

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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: **347**
裁量モードでは、次のエンティティのどれが他の人に情報アクセスを許可することを許可されていますか？
A. セキュリティマネージャー
B. グループリーダー
C. ユーザー
D. マネージャー
Answer: C (メーッセージを残す**)**

最新問題: **348**
Javaは、次のセキュリティモデルに従います。
A. 最小特権
B. サンドボックス
C. CIA
D. OSI
Answer: B (メーッセージを残す**)**
説明/参照：
Explanation:
Javaアプレットが実行されると、JVM（Java仮想マシン）は、サンドボックスと呼ばれる環境を提供する仮想マシンを作成します。この仮想マシンは、アプレットがそのアクティビティを実行する密閉された環境です。
不正解：
A：最小特権POLP）の原則は、通常の機能を可能にする最小レベルへのアクセスを制限することです。Javaは、POLPモデルではなく、サンドボックスモデルを使用します。
C :シンプルですが広く適用できるセキュリティモデルはCIAトライアドです。機密性、完全性、可用性を表す。あらゆる種類の安全なシステムで保証されるべき3つの重要な原則。JavaはCIAセキュリティモデルを使用しません。

D :OSI（Open Systems Interconnection）は、アプリケーションがネットワークを介して通信する方法の参照モデルです。OSIはJavaとは関係ありません。
参照：
コンラッド、エリック、セスミゼナル、ジョシュアフェルドマン、CISSP学習ガイド、第2版、Syngress、ウォルサム、
2012年、p。1154

最新問題: **349**
パーソナルコンピュータの領域で非同期通信の整合性を向上させるために、Microcom Networking Protocol（MNP）は、次のような非常に効果的な通信エラー制御技術を使用します。
A. エコープレックス。
B. 巡回冗長検査。
C. チェックサム。
D. 垂直冗長検査。
Answer: A (メーッセージを残す**)**

最新問題: **350**
次の共通データネットワークサービスのうち、電子メールゲートウェイデバイスを介して内部または外部で電子メールを送受信するために使用されるのはどれですか？
A. ファイルサービス。
B. メールサービス。
C. 印刷サービス。
D. クライアント/サーバーサービス。
Answer: B (メーッセージを残す**)**
メールサービスは、電子メールゲートウェイデバイスを介して内部または外部で電子メールを送受信します。
出典 :KRUTZ、Ronald L.＆VINES、Russel D.、CISSP準備ガイド :マスタリング
コンピュータセキュリティの10のドメイン、2001年、John Wiley＆Sons、99ページ。

最新問題: **351**
次のうち、802.11ワイヤレスローカルエリアネットワークが使用するコンピュータネットワークの多元接続方法はどれですか。
A. CSMA / CA
B. CSMA / CD
C. 802.11は複数のアクセス方法をサポートしていません
D. 802.11 RTS / CTS Exchange
Answer: (解答を表示する**)**
ネットワークハブがネットワークで一般的に使用されていた時代には、送信されたすべてのパケットはすべてのステーションで受信されましたが、意図された宛先MACアドレスのみがリッス

ンすることになっています。 スニファはすべての宛先MACアドレスに応答し、検査のためにそれらのパケットを保存できます。）ハブはセキュリティまたはプライバシーを提供しませんでした。ノードの数とトラフィックの量が増えると、ネットワーク上でフレームの衝突が大量に発生するため、ハブネットワークはスケーラブルではないことが判明しました。衝突とは、2つのステーションが同時に回線上で話し、送信される両方のフレームが損傷しているため、再送信する必要がある場合です。
ワイヤレスネットワークは、すべてのステーションがネットワーク上で送信されるすべてのトラフィックを 見る」ため、ハブネットワークに似ています。この状況は、CSMA/CAアクセス方式によって軽減されます。CSMA / CAを使用すると、送信を希望するノードはネットワークをリッスンして、誰かが送信しているかどうかを確認し、送信している場合は待機します。それ以外の場合は、トラフィックを送信します。
CSMA / CA キャリアセンス多元接続/衝突回避）は、802.11ネットワークでのキャリア伝送用のプロトコルです。衝突が発生した後の送信を処理するCSMA/CD Carrier Sense Multiple Access / Collision Detect）とは異なり、CSMA/CAは衝突が発生する前に衝突を防ぐように機能します。CSMA / CAでは、ノードが送信されるパケットを受信するとすぐに、チャネルがクリアされていることを確認します その時点で他のノードは送信していません）。チャネルがクリアされている場合、パケットが送信されます。チャネルがクリアされていない場合、ノードはランダムに選択された期間待機してから、チャネルがクリアされているかどうかを再度確認します。この期間はバックオフ係数と呼ばれ、バックオフカウンターによってカウントダウンされます。バックオフカウンタがゼロに達したときにチャネルがクリアされている場合、ノードはパケットを送信します。バックオフカウンタがゼロに達したときにチャネルがクリアされていない場合、バックオフ係数が再度設定され、プロセスが繰り返されます。
次の回答は正しくありません。CSMA/CD :CSMA / CDは、遅延の問題のためにワイヤレスネットワークを十分にサポートしておらず、 隠れノード」は他のノードには表示されませんが、AP-アクセスポイントには表示されます。これは、制御フレームが受信されないため、衝突検出が機能しないことを意味します。これは有線ネットワークでのみ使用されます。
Carrier Sense Multiple Access / Collision Detect CSMA / CD）は、イーサネットネットワークでのキャリア伝送アクセス用のプロトコルです。イーサネットでは、どのデバイスもいつでもフレームの送信を試みることができます。各デバイスは、回線がアイドル状態であり、したがって使用可能かどうかを検知します。そうである場合、デバイスは最初のフレームの送信を開始します。別のデバイスが同時に送信しようとした場合、衝突が発生したと言われ、フレームは破棄されます。次に、各デバイスはランダムな時間待機し、送信の送信に成功するまで再試行します。CSMA / CDは、IEEE802.3標準で指定されています。
802.11は複数のアクセス方法をサポートしていません :これは正しくありません。802.11ワイヤレスは、CSMA/CAを使用したワイヤレスメディアへの複数のアクセスをサポートします。
802.11 RTS / CTS交換 :これはアクセス制御方法ではなく、ノードがシグナリングを強化するためにノードによって交換される送信を要求する RTS）パケットを送信する CTS）CSMA/CAへの補足パケットです。
この質問を作成するために、次の参照が使用されました。

CEH-認定倫理的ハッカー :Sybex、Kimberly Graves-Wiley Publishing、INC 2010

最新問題: **352**
伝送制御プロトコル（TCP）とユーザーデータグラムプロトコル（UDP）に関して正しいのは次のうちどれですか？
A. TCPはコネクション型ですが、UDPはそうではありません。
B. UDPはエラー訂正を提供しますが、TCPは提供しません。
C. UDPは、TCPではなく長いメッセージに役立ちます。
D. TCPはデータの配信を保証しませんが、UDPはデータの配信を保証します。
Answer: A (メーッセージを残す)
説明/参照：
Explanation:
TCPはコネクション型プロトコルですが、UDPはコネクションレス型プロトコルです。
不正解：
B :TCPはエラー修正を提供しますが、UDPは提供しません。逆ではありません。
C :UDPはコネクションレス型プロトコルであるため、コネクション型プロトコルTCPと比較して、長いメッセージにはあまり役立ちません。
D :TCPはコネクション型プロトコルであるため、データの配信を保証しますが、UDPはコネクションレス型であるため、データ配信を保証しません。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、New York、2013、p。525

最新問題: **353**
データベースへのアクセスを維持および提供するソフトウェアを定義しているのは次のうちどれですか？
A. データベース識別システム（DBIS）
B. インターフェース定義言語システム（IDLS）
C. データベース管理システム（DBMS）
D. リレーショナルデータベース管理システム（RDBMS）
Answer: C (メーッセージを残す)

最新問題: **354**
OSIモデルのレイヤー2には、2つのサブレイヤーがあります。それらのサブレイヤーとは何ですか？また、そのレイヤーのテクノロジーを説明する2つのIEEE標準は何ですか？
A. LLCおよびMAC; IEEE802.2および802.3
B. LLCおよびMAC; IEEE802.1および802.3
C. ネットワークとMAC; IEEE802.1および802.3
D. LLCおよびMAC; IEEE802.2および802.3
Answer: (解答を表示する)
説明/参照：

Explanation:
OSI層はデータリンク層です。データリンク層は、論理リンク制御（LLC）とメディアアクセス制御（MAC）の2つの機能サブレイヤーに分かれています。
イーサネットのIEELLC仕様はIEEE802.2標準で定義されていますが、イーサネットのIEEEMAC仕様は802.3です。
不正解：
A :LCLはOSIレイヤー2のサブレイヤーではありません。
B :LCLはOSIレイヤー2のサブレイヤーではありません。
C :ネットワークはOSIレイヤー2のサブレイヤーではありません。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、New York、2013、p。528
http://en.wikipedia.org/wiki/OSI_model

最新問題: **355**
2000年1月の欧州連合電子署名指令、
高度電子署名を定義します。この署名は満たす必要があります
以下を除くすべての要件：
A. 一般的にアクセス可能で利用可能な手段を使用して作成する必要があります。
B. 署名者に一意にリンクされている必要があります。
C. データのその後の変更を検出できるように、関連するデータにリンクする必要があります。
D. 署名者を識別できる必要があります。
Answer: (解答を表示する**)**
指令は、手段が署名者の単独の管理下に維持されることを要求しています。この要件を達成するのは特に困難です。1つのアプローチは、関連するさまざまなトランザクションにさまざまなトークンまたはスマートカードを使用することです。他の答えは、公開鍵暗号で実装できるデジタル署名の典型的な特性です。

最新問題: **356**
以下のVPNトンネルに関する説明のうち正しくないものはどれですか？
A. ノード認証システムを実装することで作成できます。
B. IPSecデバイスのみを実装して作成できます。
C. 鍵と証明書の交換システムを実装することで作成できます。
D. クライアントまたはネットワークにソフトウェアまたはハードウェアエージェントをインストールすることで作成できます。
Answer: B (メーッセージを残す**)**
正解は「IPSecデバイスのみを実装することで作成できる」です。VPNの作成には、IPSec互換および非IPSec互換のデバイスが使用されます。他の3つの答えは、VPNを作成するためのすべての方法です。

最新問題: **357**

違反クリッピングレベルは、違反の追跡と分析にどのように役立ちますか？
A. クリッピングレベルは、許容可能な通常のユーザーエラーのベースラインを設定し、そのしきい値を超える違反は、違反が発生した理由の分析のために記録されます。
B. クリッピングレベルにより、セキュリティ管理者は監査証跡をカスタマイズして、セキュリティに関連すると見なされる違反のみを記録できます。
C. クリッピングレベルを使用すると、セキュリティ管理者は監査証跡をカスタマイズして、特権ステータスのユーザーアカウントにアクセスできるユーザーのアクションのみを記録できます。
D. クリッピングレベルにより、セキュリティ管理者は、違反が発生したユーザーアカウントに対して行われたセキュリティレベルのすべての低下を表示できます。
Answer: A (メーッセージを残す**)**
企業は、アクティビティが疑わしいと見なされる前に許可される特定のタイプのエラーの数に事前定義されたしきい値を設定できます。しきい値は、アラームが発生する前にユーザーがコミットするのが正常な違反アクティビティのベースラインです。このベースラインは、クリッピングレベルと呼ばれます。
以下は不正解です。
クリッピングレベルを使用すると、セキュリティ管理者は監査証跡をカスタマイズして、セキュリティに関連すると見なされる違反のみを記録できます。これは最善の答えではありません。セキュリティ関連の違反のみを記録するのではなく、すべての違反と、違反をトリガーしない可能性のある許可されたユーザーによって実行されたすべてのアクションが記録されます。これにより、事後に異常な活動や詐欺を特定できる可能性があります。
クリッピングレベルを使用すると、セキュリティ管理者は監査証跡をカスタマイズして、特権ステータスのユーザーアカウントにアクセスできるユーザーのアクションのみを記録できます。ユーザーが通常のユーザーであるか特権ユーザーであるかに関係なく、すべてのセキュリティ違反を記録する可能性があります。
クリッピングレベルを使用すると、セキュリティ管理者は、違反が発生したユーザーアカウントに対して行われたセキュリティレベルのすべての低下を表示できます。キーワード「ALL」はこの質問を間違っています。一部の違反を検出する場合がありますが、すべての違反を検出するわけではありません。たとえば、アプリケーションレベルの攻撃が検出されない場合があります。
この質問に使用される参照：
ハリス、ション（2012-10-18）。CISSPオールインワン試験ガイド、第6版（p.1239）。マグロウ-丘。キンドル版。
と
TIPTON、Hal、（ISC）2、CISSP試験プレゼンテーションの概要。

最新問題**: 358**
企業は、許可されていないユーザーからコンピューターを保護するために2要素認証（2FA）を実装したいと考えています。最も安全な認証手段を提供し、設定された基準を満たすソリューションはどれですか？
A. ユーザー名と暗証番号（PIN）

B. ショートメッセージサービス（SMS）とスマートフォン認証システム
C. 指紋および網膜スキャナー
D. ハードウェアトークンとパスワード
Answer: D (メーッセージを残す**)**

最新問題**: 359**
事業継続計画はどのくらいの頻度で見直されるべきですか？
A. 少なくとも月に1回
B. 少なくとも6か月ごと
C. 少なくとも年に1回
D. 少なくとも四半期ごと
Answer: C (メーッセージを残す**)**
SP 800-34Rev.1に記載されているとおり。
効果を上げるには、計画をシステムを正確に反映した準備状態に維持する必要があります
要件、手順、組織構造、およびポリシー。間に
SDLCの運用/保守フェーズでは、情報システムは頻繁に変更されます
ビジネスニーズの変化、テクノロジーのアップグレード、または新しい内部または外部ポリシー
のため。
原則として、組織で計画の正確性と完全性を確認する必要があります–
定義された頻度（試験の目的で少なくとも年に1回）または重要な場合はいつでも
計画の任意の要素に変更が発生します。連絡先リストなどの特定の要素には、
より頻繁なレビュー。
上で指定したように、2つの良い答えがある可能性があることを忘れないでください。年に一度また
はいつでも
計画に大幅な変更が発生します。もちろん、内に提示された2つのうちの1つだけを取得します
あなたが試験します。
この質問に使用される参照：
NISTSP800-34リビジョン1

最新問題**: 360**
次のうち、証拠の適切なライフサイクルはどれですか？
A. コレクション、保管、法廷に存在、破壊
B. 収集、輸送、保管、所有者への返却
C. 収集、法廷での存在、輸送、所有者への返還
D. 収集、分析、保管、法廷での提示、所有者への返還
E. 収集、保管、輸送、法廷での提示、所有者への返却
Answer: D (メーッセージを残す**)**
証拠のライフサイクルには、収集、分析、保管、法廷での提示、所有者への返還が含まれます。

最新問題**: 361**

システムの再認証と再認定が必要な主な理由は次のうちどれですか？
A. すべてのセキュリティ問題が解決されたことをソフトウェア開発チームに保証するため
B. セキュリティチームが実装と本番用の新しいシステムを受け入れるか拒否するのを支援するため
C. データ所有者が将来の機密性と重要度を決定するのを支援するため
D. セキュリティ保護が組織のセキュリティポリシーに受け入れられることを確認するため
Answer: D (メーッセージを残す**)**

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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**: 362**
以下のネットワーク設計では、請負業者にインターネットと認定エンタープライズサービスへのアクセスを提供するワイヤレスアクセスポイント（WAP）を展開するための最も安全なローカルエリアネットワーク（LAN）セグメントはどこにありますか？

Internet
LAN 3
Firewall
LAN 1
LAN 4
DNS Server
Firewall
Ecommerce Server
LAN 2
Database Server

Answer:

説明
LAN 4

最新問題: **363**
システムの所有者は、システムがその仕様に従って動作することを確信している必要があります。
これは次のように呼ばれます：
A. 整合性
B. 説明責任
C. 保証
D. 可用性
Answer: C (メーッセージを残す**)**
システムの所有者は、システムがその仕様に従って動作することを確信している必要があります。
これは保証と呼ばれます
次の答えは正しくありません。
威厳
説明責任
可用性
この質問を作成するために、次の参照が使用されました。

倫理的なハッキング対策
倫理的ハッキング入門
オレンジブック

最新問題: **364**
次のうち、ネットワークケーブルタイプではないものはどれですか？
A. 同軸
B. トークンリング
C. ツイストペア
D. 光ファイバー
Answer: B (メーッセージを残す**)**
正解のトークンリング。トークンリングはLANメディアアクセス方式であり、ケーブルタイプではありません。

最新問題: **365**
オフサイトのハードウェアバックアップ機能を定期的にテストする主な目的は何ですか？
A. プログラムとシステムのドキュメントを最新の状態に保つため
B. 緊急時対応施設の継続的な互換性を確保するため
C. 詳細な緊急時対応計画を作成する必要をなくすため
D. データベース内のデータの整合性を確保するため
Answer: B (メーッセージを残す**)**

最新問題: **366**
不適切なコンピュータアクティビティは、次のように説明できます。
A. 通常のシステムユーザーが利用できるリソースを介したデータの清掃。
B. 利益または不正開示のための情報または企業秘密の盗難。
C. 仕事の行動または解雇の理由となる可能性のあるコンピューターの動作。
D. オペレーターの訓練が不足しているにもかかわらず、意図せずに損失が発生した。
Answer: C (メーッセージを残す**)**
正解は「仕事の行動や解雇の理由となる可能性のあるコンピューターの行動」です。説明されているすべての活動は、不適切な活動の幅広いカテゴリで考慮されていますが、これは
説明は、不適切なより狭いカテゴリを定義するために使用されます
活動。
「オペレーターの訓練が不足しているにもかかわらず、意図せずに損失が発生した」と回答します。偶発的な損失として定義されます。
「利益または不正開示のための情報または企業秘密の盗難」に回答してください。意図的に違法なコンピュータ活動と見なされます。
「通常のシステムユーザーが利用できるリソースを介したデータスカベンジング」とは、ユーザーが利用できる一般的なツールやユーティリティを使用したデータスカベンジング攻撃の一種であるキーボード攻撃です。

最新問題: **367**
管理者によるシステムの全体的なセキュリティの妥当性の正式な承認とは何ですか？
A. 認証
B. 受け入れ
C. 認定
D. 評価
Answer: C (メーッセージを残す**)**
説明/参照：
Explanation:
認定とは、本番環境にソフトウェアまたはシステムを実装するための管理者による承認です。この承認は、暫定的または完全なもののいずれかです。以下は不正解です。
認定が正しくありません。認証は、選択された一連の標準またはポリシーに対してソフトウェアまたはシステムのセキュリティスタンスを評価するプロセスです。認証とは、製品の技術的評価です。
これは認定に先行する可能性がありますが、必須の前兆ではありません。受け入れが正しくありません。この用語は、ソフトウェアまたはシステムの一部が一連の機能レベルまたはサービスレベルの基準を満たしている（新しい給与システムがその受け入れテストに合格している）という認識として使用されることがあります。この文脈では、認証がより適切な用語です。評価が正しくありません。評価は確かに認証プロセスの一部ですが、それは質問に対する最良の答えではありません。
参考資料：ISC2のCBKの公式学習ガイド、559～560ページAIO3、314～317ページAIOv4セキュリティアーキテクチャおよび設計（369～372ページ）AIOv5セキュリティアーキテクチャおよび設計（370～370ページ）
372）

最新問題: **368**
自己監査と独立監査の本質的な違いは何ですか？
A. 使用したツール
B. 結果
C. 客観性
D. 能力
Answer: C (メーッセージを残す**)**
運用の保証を維持するために、組織は2つの基本的な方法を使用します。
システムの監査と監視。監視とは継続的な活動を指しますが、監査は1回限りまたは定期的なイベントであり、内部または外部のいずれかになります。自己監査と独立監査の本質的な違いは客観性であり、したがって間接的に監査の結果に影響を及ぼします。内部監査人と外部監査人は同じレベルの能力を持ち、同じツールを使用できる必要があります。
出典：SWANSON、Marianne＆GUTTMAN、Barbara、National Institute of Standards、Technology（NIST）、NIST Special Publication 800-14、一般的に受け入れられている原則および

情報技術システムを保護するための慣行、1996年9月 25ページ）。

最新問題: **369**
VLANに関して正しい説明は次のうちどれですか。
A. クローズドVLAN構成は、最も安全性の低いVLAN構成です。
B. プライベートポートスイッチングと組み合わせて実装すると、VLANの安全性が低下します。
C. VLANは、論理的にではなく、物理的にセグメント化されたネットワークです。
D. VLANは、フラッディングをVLANに含まれるポートのみに制限します。
Answer: D (メーッセージを残す**)**
仮想ローカルエリアネットワーク（VLAN）を使用すると、同じスイッチまたは異なるスイッチのポートをグループ化して、トラフィックをそのグループのメンバーのみに制限し、ブロードキャスト、ユニキャスト、およびマルチキャストのトラフィックを制限できます。VLANは物理的ではなく論理的にセグメント化されているため、「VLANは論理的にではなく、物理的にセグメント化されたネットワークです」という回答は正しくありません。「プライベートポートスイッチングと組み合わせて実装するとVLANの安全性が低下します」という回答は正しくありません。
VLANがプライベートポートまたはシングルユーザースイッチングで実装されている場合、ブロードキャストの脆弱性が最小限に抑えられるため、かなり厳格なセキュリティが提供されます。回答「クローズドVLAN構成は最も安全性の低いVLAN構成です」は正しくありません。クローズドVLANは、ネットワークアクセスのレベルを決定するための許可パラメータが割り当てられている中央認証サーバーのアクセス制御リストに対してユーザーを認証するためです。出典：Catalyst 5000シリーズインストールガイド（Cisco Systems）およびMariana Smithによる仮想LAN（McGraw-Hill、1998年）。

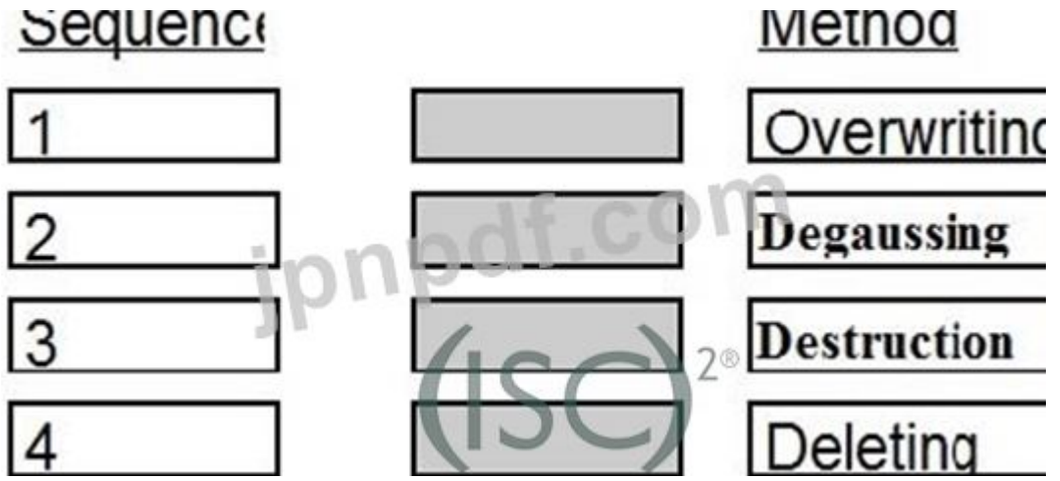
最新問題: **370**
次のうち、ユーザープロビジョニングの一部ではないものはどれですか？
A. ユーザーアカウントの作成と非アクティブ化
B. ビジネスプロセスの実装
C. ユーザーオブジェクトと属性のメンテナンスと非アクティブ化
D. ユーザー管理の委任
Answer: B (メーッセージを残す**)**
ユーザープロビジョニングとは、ビジネスプロセスに応じて、1つ以上のシステム、ディレクトリ、またはアプリケーションに存在するユーザーオブジェクトと属性の作成、保守、および非アクティブ化を指します。ユーザープロビジョニングソフトウェアには、次のコンポーネントの1つ以上が含まれる場合があります。変更
伝播、セルフサービスワークフロー、統合ユーザー管理、委任ユーザー
管理、およびフェデレーション変更管理。
ユーザーオブジェクトは、従業員、請負業者、ベンダー、パートナー、顧客、またはその他を表す場合があります
サービスの受信者。

サービスには、電子メール、データベースへのアクセス、ファイルサーバーまたはメインフレームへのアクセスが含まれる場合があります。
等々
次の答えはすべて間違った答えです。
ユーザーアカウントの作成と非アクティブ化
ユーザーオブジェクトと属性のメンテナンスと非アクティブ化
ユーザー管理の委任
この質問を作成するために、次の参照が使用されました。
ハリス、ション（2012-10-18）。CISSPオールインワン試験ガイド、第6版（p.179）。マグロウヒル。キンドル版。

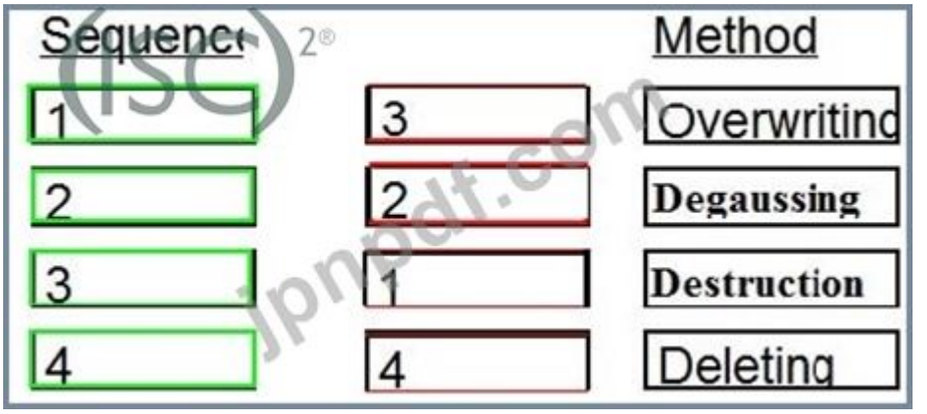
最新問題: **371**
攻撃を受けやすいことがわかっているWebベースのアプリケーションは、現在、上級開発者によってレビューされています。組織は、このアプリケーションが特にインジェクション攻撃の影響を受けにくいことを確認したいと考えています。組織の状況に最適な戦略はどれですか。
A. オペレーティングシステム（OS）のキャッシュまたはメモリにデータを保持するバッファに機密データを保存します。
B. 特権アクセスまたはログオン資格情報のハードコーディングを制限します。
C. 暗号化されていない機密データをバックエンドに保存しないでください。
D. レンダリングのために処理される前に、入力をホワイトリストに登録し、出力をエンコードまたはエスケープします。
Answer: (解答を表示する**)**

最新問題: **372**
ソフトウェアセキュリティテストの全体的な目標は何ですか？
A. すべてのソフトウェア機能が指定どおりに実行されるようにする
B. ソフトウェアの主要なセキュリティ機能を特定する
C. ソフトウェアシステム内の脆弱性を減らす
D. ソフトウェア開発をより機敏にする
Answer: (解答を表示する**)**

最新問題: **373**
ドラッグドロップ
磁気媒体にデータが残るリスクを減らすために、BEST（1）からWORST（4）の順に次の方法を並べてください。



Answer:



最新問題: **374**

次の回答のうち、ネットワークベースのIDSまたはIPSシステムに最も重大な脅威をもたらすものはどれですか？

A. 暗号化されたトラフィック

B. 複雑なIDS/IPS署名構文

C. デジタル署名されたネットワークパケット

D. 分離されたVLAN

Answer: A (メーッセージを残す**)**

考察：暗号化されたネットワークパケットは、ネットワークを簡単に（または迅速に）デコードおよび検査できないため、効果的なIDS/IPS計画に最大の脅威をもたらします。

IDSは暗号化されたパケットを調べて脅威があるかどうかを判断できないため、ほとんどの場合、トラフィックは潜在的な脅威とともに転送されるだけです。

企業がネットワークトラフィックの検査サービスを提供し、すべてのネットワークトラフィックのプロキシサーバーのように機能する業界があります。

証明書のコピーを送信するだけで、トラフィックをデコードできます。これは、連邦法に違反したり、インサイダー取引のために連邦捜査官に訴えられたりすると、ビジネスが崩壊する可能性がある金融業界では一般的です。

外部の会社は、潜在的な責任について、ネットワークとの間で送受信されるすべてのネットワークトラフィックを調べます。

次の答えは正しくありません。-複雑なIDS/IPS署名構文 :IDS / IPS署名は複雑になる可能性がありますが、これはIDS/IPSシステムの機能に対する最も重大な脅威ではありません。
-デジタル署名されたネットワークパケット：危険なネットワークトラフィックを探しているIDS / IPSシステムにとって脅威ではないため、これは不正解です。何よりも、送信する各ネットワークパケットにデジタル署名することは一般的ではないためです。
-分離されたVLAN :これは正解ではありませんが、VLANは、危険なトラフィックを検出するIDS/IPSシステムに対する障壁となる可能性があります。VLANとIDS/IPSシステムには簡単な解決策があり、そのVLANにIDS / IPSセンサーを配置し、そのVLANをIDS/IPS管理システムに送信するように設定するだけです。
この質問を作成するために、次の参照が使用されました。
グレッグ、マイケル; ヘインズ、ビリー（2012-02-16）。CASP :CompTIA Advanced Security Practitioner
学習ガイド認定コースウェア：試験CAS-001（Pg。138）Wiley。キンドル版。

最新問題**: 375**
新しいログオンごとに新しいパスワードが必要になるため、どのタイプのパスワードが最大のセキュリティを提供しますか？
A. ワンタイムまたは動的パスワード
B. わかりやすいパスワード
C. 静的パスワード
D. パスフレーズ
Answer: A (メーッセージを残す**)**
「ワンタイムパスワード」は、新しいログオンごとに新しいパスワードが必要になるため、最大限のセキュリティを提供します。
出典 :KRUTZ、Ronald L.＆VINES、Russel D.、CISSP準備ガイド :マスタリングコンピュータセキュリティの10のドメイン、2001年、John Wiley＆Sons、36ページ

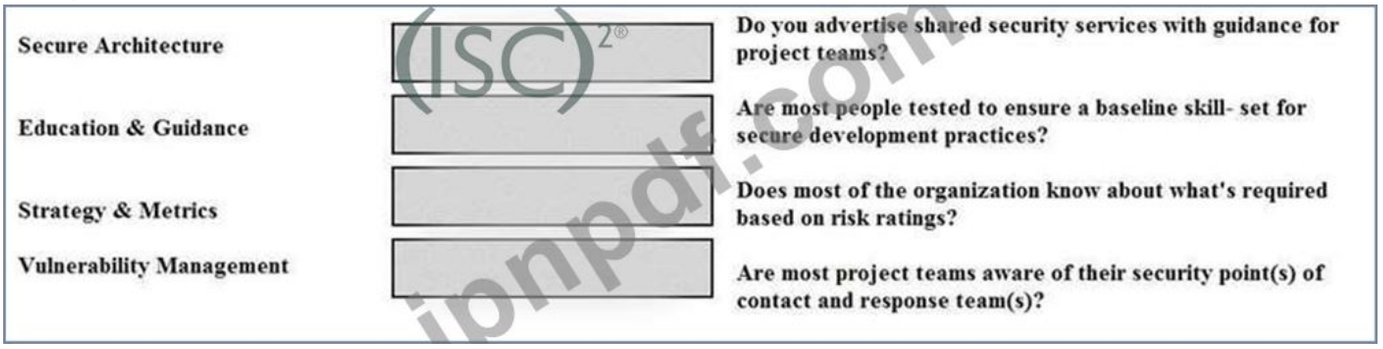
最新問題**: 376**
以下のどの項目がフェデレーションID標準ですか？
A. ライトウェイトディレクトリアクセスプロトコル（LDAP）
B. セキュリティアサーションマークアップ言語（SAML）
C. Kerberos
D. 802.11i
Answer: B (メーッセージを残す**)**

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

こちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (1533330%OFF問題集溶と正解付きで 30%ｗ特別割引コード: Freepdfdumps)

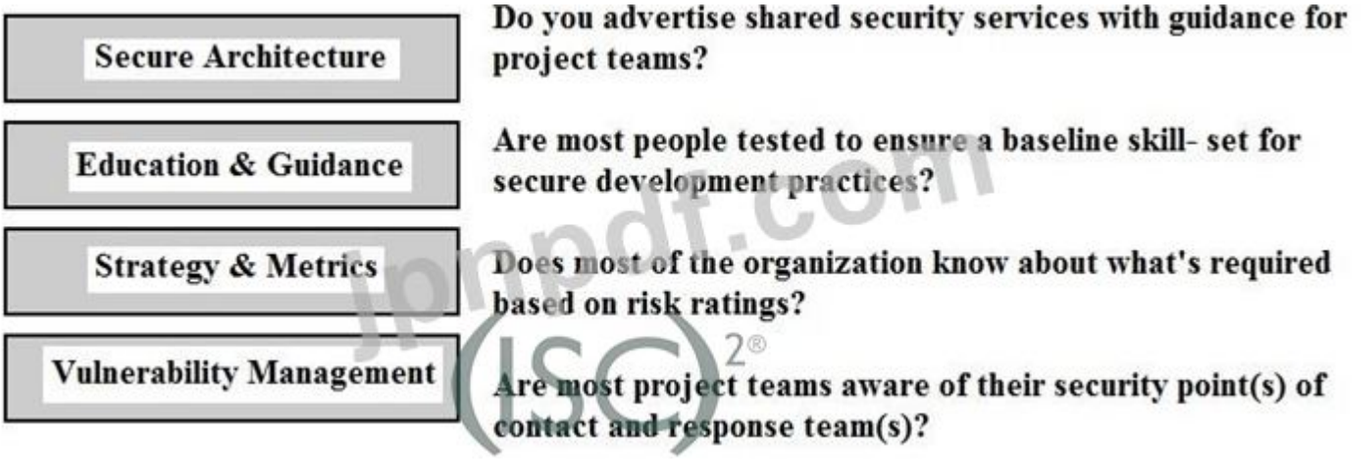
最新問題: 377

Software Assurance Maturity Model（SAMM）のガバナンスドメインの評価質問に目的を一致させます。



Answer:

説明



最新問題: 378

次のうち、電子メールメッセージの機密性を提供するものはどれですか？

A. 送信者が秘密鍵で暗号化します。

B. 送信者が公開鍵で暗号化します。

C. 送信者は受信者の公開鍵で暗号化します。

D. 送信者は受信者の秘密鍵で暗号化します。

Answer: C (メーッセージを残す)

説明/参照：
Explanation:
公開鍵を使用して暗号化されたメッセージは、対応する秘密鍵を使用してのみ復号化できます。受信者は、受信者の秘密鍵を所有している唯一の人物である必要があります。受信者の公開鍵は自由に配布できます。
したがって、送信者が受信者の公開鍵を使用してメッセージを暗号化すると、送信者は、受信者がメッセージを復号化できる唯一の人物であることがわかります。これにより、メッセージの機密性が確保されます。
不正解：
A：公開鍵は自由に配布できます。送信者が自分の秘密鍵を使用してメッセージを暗号化すると、送信者の公開鍵を所有している人は誰でもメッセージを復号化できます。これは機密性を提供しません。
B：公開鍵を使用して暗号化されたメッセージは、対応する秘密鍵を使用してのみ復号化できます。送信者が自分の公開鍵を使用してメッセージを暗号化する場合、自分の公開鍵に対応する秘密鍵を所有しているのは自分だけであるため、送信者だけがメッセージを復号化できます。
D：受信者は、受信者の秘密鍵を所有している唯一の人物である必要があります。送信者は、受信者の秘密鍵を所有してはなりません。

最新問題: **379**
セキュリティエンジニアは、サードパーティベンダー向けの顧客関係管理（CRM）アプリケーションを設計しています。システム開発ライフサイクル（SDLC）のどのフェーズで、データ感度評価を実施することが最も有益でしょうか？
A. 列挙
B. 開発/買収
C. 運用/保守
D. 開始
Answer: D (メーッセージを残す**)**

最新問題: **380**
変更管理を実装する主な理由は何ですか？
A. 環境の変化に対する説明責任を確保する
B. 環境へのリリースを認証および承認します
C. システム変更のバージョンロールバックを提供する
D. すべての申請が承認されていることを確認します
Answer: A (メーッセージを残す**)**

最新問題: **381**
必要なときに必要な場所でデータにアクセスできることを確認するのは、次のうちどれですか。
A. 守秘義務
B. 整合性

C. 受容性
D. 可用性
Answer: D (メーッセージを残す**)**
可用性とは、必要なときに必要な場所でデータにアクセスできるようにすることです。
出典 :KRUTZ、Ronald L.＆VINES、Russel D.、CISSP準備ガイド :マスタリング
コンピュータセキュリティの10のドメイン、2001年、John Wiley＆Sons、59ページ。

最新問題**: 382**
次の組織のうち、連邦情報処理標準 （FIPS）を作成および公開しているのはどれですか？
A. National Computer Security Center （NCSC）
B. 米国国立標準技術研究所 （NIST）
C. 国家安全保障局 （NSA）
D. 米国規格協会 （ANSI）
Answer: B (メーッセージを残す**)**
説明/参照：
Explanation:
連邦情報処理標準 （FIPS）は、米国連邦の省庁が採用および使用するための規格であり、情報技術研究所内で開発され、米国国立標準技術研究所 （NIST）によって発行されています。商務省。FIPSは、非軍事政府機関内で、および政府機関と協力する政府の請負業者やベンダーが使用するための文書処理、暗号化アルゴリズム、およびその他の情報技術標準について説明しています。この規格は、情報技術 （IT）の特定のトピックを対象としており、共通レベルの品質または相互運用性の実現に努めています。
不正解：
A :National Computer Security Center （NCSC）は、連邦情報処理標準 （FIPS）を作成または公開していません。
C：国家安全保障局NSA）は、連邦情報処理標準 （FIPS）を作成または公開していません。
D：米国規格協会ANSI）は、連邦情報処理標準 （FIPS）を作成または公開していません。
参考文献」
http://whatis.techtarget.com/definition/Federal-Information-Processing-Standards-FIPS

最新問題**: 383**
データベース内のデータの正規化には、次のうちどれを除いてすべてまたは一部を含めることができますか？
A. 同じテーブルから重複する列を削除します。
B. キー全体に依存するフィールドとは別のテーブルにフィールドを配置することにより、部分的なキーへの機能依存性を排除します
C. 非キーフィールドを別のテーブルに配置することにより、非キーフィールドへの機能依存性を排除します。このレベルでは、すべての非キーフィールドは主キーに依存しています。
D. 別々のテーブルに配置することにより、重複するキーフィールドを排除します。
Answer: D (メーッセージを残す**)**

説明/参照：
Explanation:
データベース内のデータを正規化しても、重複するキーフィールドを別々のテーブルに配置して排除することはできません。
すべてのテーブルが繰り返しグループのない2次元である場合、エンティティは第一正規形（1NF）になります。
基になるすべてのドメインにアトミック値のみが含まれている場合、行は第一正規形（1NF）になります。1NFは、グループを別々のテーブルに配置し、それらを1対多の関係で接続することにより、グループの繰り返しを排除します。関連する属性のセットごとに個別のテーブルを作成し、主キーを使用して各レコードを一意に識別します。
同じテーブルから重複する列を削除します。
- 関連データのグループごとに個別のテーブルを作成し、一意の列またはセットで各行を識別します
- 列の数（主キー）。

エンティティは、第1正規形（1NF）であるという要件を満たし、さらに次の要件を満たしている場合、第2正規形（2NF）になります。
複合主キーはありません。主キーを次のように細分化できないことを意味します
- 個別の論理エンティティ。
- すべての非キー列は、主キー全体に機能的に依存しています。
- 行が第1正規形であり、すべての非キー属性が完全にある場合に限り、行は第2正規形になります。
- キーに依存します。

2NFは、フィールドを別のテーブルに配置することにより、部分キーへの機能依存性を排除します。
- キー全体に依存するもの。例は、交差するエンティティを使用して多くの：多く の関係を解決することです

エンティティは、第2正規形（2NF）であるという要件を満たし、さらに次の要件を満たしている場合、第3正規形（3NF）になります。
非キーフィールドへの機能依存性は、それらを別のテーブルに配置することで排除されます。これで
- レベルでは、すべての非キーフィールドは主キーに依存しています。
- 行が第2正規形であり、属性が第2正規形でない場合に限り、行は第3正規形になります。
- 主キーの説明に貢献することは別のテーブルに移動されます。例として、ルックアップテーブルの作成があります。

不正解：
A :データベース内のデータを正規化すると、同じテーブルから重複する列が削除されます。
B :データベース内のデータを正規化すると、キー全体に依存するフィールドとは別のテーブルにフィールドを配置することで、部分的なキーへの機能的な依存関係が排除されます。

C :データベース内のデータを正規化すると、キー以外のフィールドを別のテーブルに配置することで、機能的な依存関係がなくなります。
参照：
http://psoug.org/reference/normalization.html
http://searchsqlserver.techtarget.com/definition/normalization?vgnextfmt=print

最新問題: **384**
エンタープライズIDおよびアクセス管理（IAM）ソリューションを実装するメリットは次のうちどれですか？
A. データの機密性が向上します。
B. 職務の分離は自動的に実施されます。
C. 孤立したアカウントに関連するリスクが軽減されます。
D. パスワード要件が簡素化されます。
Answer: D (メーッセージを残す**)**

最新問題: **385**
次のうち、本人拒否率と呼ばれる生体認証エラーのタイプを説明するのはどれですか？
A. タイプIエラー
B. タイプIIエラー
C. タイプIIIエラー
D. CERエラー
Answer: A (メーッセージを残す**)**
生体認証システムが許可された個人を拒否する場合、それはタイプIエラーと呼ばれます。
システムが拒否されるべき（誤検知）詐欺師を受け入れる場合、それはタイプIIと呼ばれます
エラー。
パーセンテージで表されるクロスオーバーエラー率（CER）は、falseが発生するポイントを表します
拒否（タイプI）率は、誤受け入れ（タイプII）率と同じです。
タイプIIIのエラーは定義されておらず、この場合は単に気を散らすものです。一部の人々はこれにだまされます
バイオメトリクスがタイプIII認証である認証要素について考えているからです
要素。
認証要素と生体認証エラーを混同しないように注意してください。3つの認証要素は次のとおりです。
タイプ1あなたが知っていること
タイプ2あなたが持っている何か
タイプ3あなたが何か
この質問に使用される参照：
HARRIS、ション、オールインワンCISSP認定試験ガイド、McGraw-Hill / Osborne、2002年、章
4 :アクセス制御（128ページ）。

と
https://pciguru.wordpress.com/2010/05/01/one-two-and-three-factor-authentication/

最新問題: **386**
次のうち、分散データ処理（DDP）アプローチの特徴ではないものはどれですか？
A. サイトが次のようになった場合にコンピューティングの代替手段を提供できる複数の処理場所で構成されます
動作不能。
B. 地理的に離れた複数の場所に保存されているデータは、ユーザーが簡単に利用できます。
C. ユーザーから処理リソースまでの距離はユーザーに対して透過的です。
D. ネットワークシステムによりセキュリティが強化されています。
Answer: (解答を表示する**)**
ネットワークに関連する脆弱性と、コンピューティングリソースへの不正アクセスが発生する可能性のある多くの場所があるため、分散システムではセキュリティがより重要になります。他の答えは、DDPアーキテクチャの特性です。

最新問題: **387**
次のうち、Diffie-に基づくキー確立プロトコルとして定義されているのはどれですか
ヘルマンアルゴリズムはIPsecに提案されましたが、IKEに取って代わられましたか？
A. Diffie-Hellman鍵交換プロトコル
B. インターネットセキュリティアソシエーションおよびキー管理プロトコル（ISAKMP）
C. インターネットプロトコルの単純なキー管理（SKIP）
D. オークリー
Answer: (解答を表示する**)**
RFC 2828（Internet Security Glossary）は、OAKLEYをDiffie-に基づくキー確立プロトコル（IPsecで提案されているが、IKEに取って代わられている）として定義しています。
ヘルマンアルゴリズムであり、ISAKMPの互換性のあるコンポーネントになるように設計されています。
ISAKMPは、特定のキー生成技術、キー確立プロトコル、暗号化アルゴリズム、または認証メカニズムの詳細に関係なく、セキュリティアソシエーションをネゴシエート、確立、変更、および削除し、キー生成および認証データを交換するためのインターネットIPsecプロトコルです。
SKIPは、ハイブリッド暗号化を使用して、IPパケット内のデータの暗号化に使用されるセッションキーを伝達するキー配布プロトコルです。
ISAKMPは、認証とキー交換のためのフレームワークを提供しますが、それらを定義しません。ISAKMPは、鍵交換に依存しないように設計されています。つまり、さまざまな鍵交換をサポートするように設計されています。
OakleyとSKEMEはそれぞれ、認証された鍵交換を確立する方法を定義しています。
これには、ペイロードの構築、ペイロードが運ぶ情報、それらが処理される順序、およびそれらがどのように使用されるかが含まれます。

Oakleyは、モードと呼ばれる一連のキー交換について説明し、それぞれが提供するサービスの詳細を説明します（たとえば、キーの完全転送秘密、ID保護、認証）。
SKEMEは、匿名性、否認可能性、および迅速な鍵更新を提供する、用途の広い鍵交換技術について説明しています。
RFC 2049は、ISAKMPで使用するための認証済みキーイングマテリアルを取得するために、Oakleyの一部とSKEMEの一部をISAKMPと組み合わせて使用し、IETFIPsecDOIのAHやESPなどの他のセキュリティアソシエーションのためにIKEプロトコルを記述しています。
Oakleyは「モード」を定義しますが、ISAKMPは「フェーズ」を定義します。2つの関係は非常に単純であり、IKEは2つのフェーズのいずれかで動作するモードとして異なる交換を提供します。
フェーズ1では、2つのISAKMPピアが、通信するための安全な認証済みチャネルを確立します。これはISAKMPセキュリティアソシエーション（SA）と呼ばれます。「メインモード」と「アグレッシブモード」はそれぞれフェーズ1の交換を行います。「メインモード」と「アグレッシブモード」は、フェーズ1でのみ使用する必要があります。
フェーズ2では、IPsecなどのサービス、またはキーマテリアルやパラメータネゴシエーションを必要とするその他のサービスに代わってセキュリティアソシエーションがネゴシエートされます。「クイックモード」は、フェーズ2の交換を実行します。「クイックモード」は、フェーズ2でのみ使用する必要があります。
参照：
CISSP：JamesによるCertified Information Systems Security Professional Study Guide
Michael Stewart、Ed Tittel、Mike Chappl、397ページ
RFC 2049：http://www.ietf.org/rfc/rfc2409
SHIREY、Robert W.、RFC2828：Internet Security Glossary、2000年5月。
オールインワンCISSP試験ガイド、第3版、ション・ハリス、674ページ
Krutz and VinesによるCISSPおよびCAP準備ガイド、プラチナ版

最新問題: **388**
保護リングに関する次の説明のうち、間違っているものはどれですか。
A. 各リング内で動作するプロセスがアクセスできるものに関する厳密な境界と定義を提供します。
B. 内輪で動作するプログラムは、通常、特権モードで存在すると呼ばれます。
C. マルチタスクオペレーティングシステムのCIAトライアド要件をサポートします。
D. 周辺機器への直接アクセスをユーザーに提供します
Answer: D (メーッセージを残す)
コンピュータサイエンスでは、保護リングと呼ばれることが多い階層型保護ドメインは、データと機能をフォールト（フォールトトレランス）および悪意のある動作（コンピュータセキュリティ）から保護するメカニズムです。このアプローチは、機能ベースのセキュリティのアプローチとは正反対です。
コンピュータオペレーティングシステムは、リソースへのさまざまなレベルのアクセスを提供します。保護リングは、コンピュータシステムのアーキテクチャ内の2つ以上の階層レベルまたは特

権の層の1つです。これは通常、ハードウェアまたはマイクロコードレベルでさまざまなCPUモードを提供する一部のCPUアーキテクチャによってハードウェアで強制されます。
リングは、最も特権のある（最も信頼できる、通常はゼロの番号が付けられる）から最も特権の低い（最も信頼できない、通常は最大のリング番号を持つ）までの階層に配置されます。ほとんどのオペレーティングシステムでは、リング0は最も多くの特権を持つレベルであり、CPUやメモリなどの物理ハードウェアと最も直接対話します。
リング間に特別なゲートが用意されており、任意の使用を許可するのではなく、事前定義された方法で外部リングが内部リングのリソースにアクセスできるようになっています。リング間のアクセスを正しくゲーティングすると、あるリングまたは特権レベルのプログラムが別のリングのプログラム用のリソースを悪用するのを防ぐことで、セキュリティを向上させることができます。たとえば、リング3でユーザープログラムとして実行されているスパイウェアは、ハードウェアアクセスがデバイスドライバー用に予約されたリング1機能である必要があるため、ユーザーに通知せずにWebカメラをオンにしないようにする必要があります。番号の大きいリングで実行されているWebブラウザなどのプログラムは、ネットワークへのアクセスを要求する必要があります。これは、番号の小さいリングに制限されているリソースです。 それらは、各リング内で機能するプロセスについての
厳密な境界と定義を提供します
「アクセスできます」は正しくありません。これは、実際にはリング保護システムの特徴の1つです。
「内輪で動作するプログラムは、通常、特権モードで存在すると呼ばれます」は
正しくない。これは、実際にはリング保護システムの特徴の1つです。
「マルチタスクオペレーティングシステムのCIAトライアド要件をサポートしています」は正しくありません。これは
事実、リング保護システムの特徴の1つです。
この質問に使用される参照：
CBK、pp.310-311
AIO3、pp.253-256
AIOv4セキュリティアーキテクチャと設計（308〜310ページ）
AIOv5セキュリティアーキテクチャと設計（309〜312ページ）

最新問題: **389**
大企業では、システム管理者は、役割ベースのアクセス制御（RBAC）を使用してユーザーにファイルへのアクセスを割り当てる必要があります。どのオプションがRBACの例ですか？
A. グループメンバーシップに基づいてユーザーがファイルにアクセスできるようにする
B. ファイルタイプに基づいてユーザーがファイルにアクセスできるようにする
C. ユーザー名に基づいてユーザーがファイルにアクセスできるようにする
D. アクセス時のユーザーの場所に基づいてユーザーがファイルにアクセスできるようにする
Answer: A (メーッセージを残す**)**

最新問題: **390**
次のうち、秘密鍵暗号化の問題ではないものはどれですか？
A. キーの侵害により、攻撃者がなりすましを行う可能性があります
キーの所有者であるため、誤ったメッセージを読み取って送信します。
B. mユーザーのネットワーク化されたグループ。
ユーザーはm (m-1)/2キーを必要とします。
C. 認証局のセキュリティ。
D. キーの安全な配布。
Answer: C (メーッセージを残す**)**
CAは、秘密鍵暗号ではなく、公開鍵暗号で使用されます。
CAは、公開鍵が実際に特定のものに属していることを証明します
個人およびに関連する情報
個人の鍵は有効で正しいものです。CAは、個人の公開鍵と関連情報にデジタル署名することにより、この認証を達成します。認定は、他の人に公言します公開キー暗号化
を使用してこの個人にメッセージを送信したい
公開鍵が実際に意図された個人に属していること。
諮問委員会、国際電話および電信、
国際電気通信連合 (CCITT-ITU)/
国際標準化機構 (ISO)X.509認証フレームワークは、公開鍵証明書の形式を定義します。この構造の概要を図に示します。

CCITT-ITU/ ISO X.509 certificate format.

image012

回答 「ユーザーのペアごとに別々のキーを持つm人のユーザーのネットワーク化されたグループには、m (m-1)/ 2キーが必要です」は、秘密鍵暗号化の重要な問題です。したがって、それは正解ではありません。m人のユーザーのネットワークの中で、各ユーザーがネットワーク上の他のすべてのユーザーと安全に通信したい場合は、潜在的なユーザーのペアごとに秘密鍵が必要です。

この概念は、図に示すように5人のユーザーで説明できます。

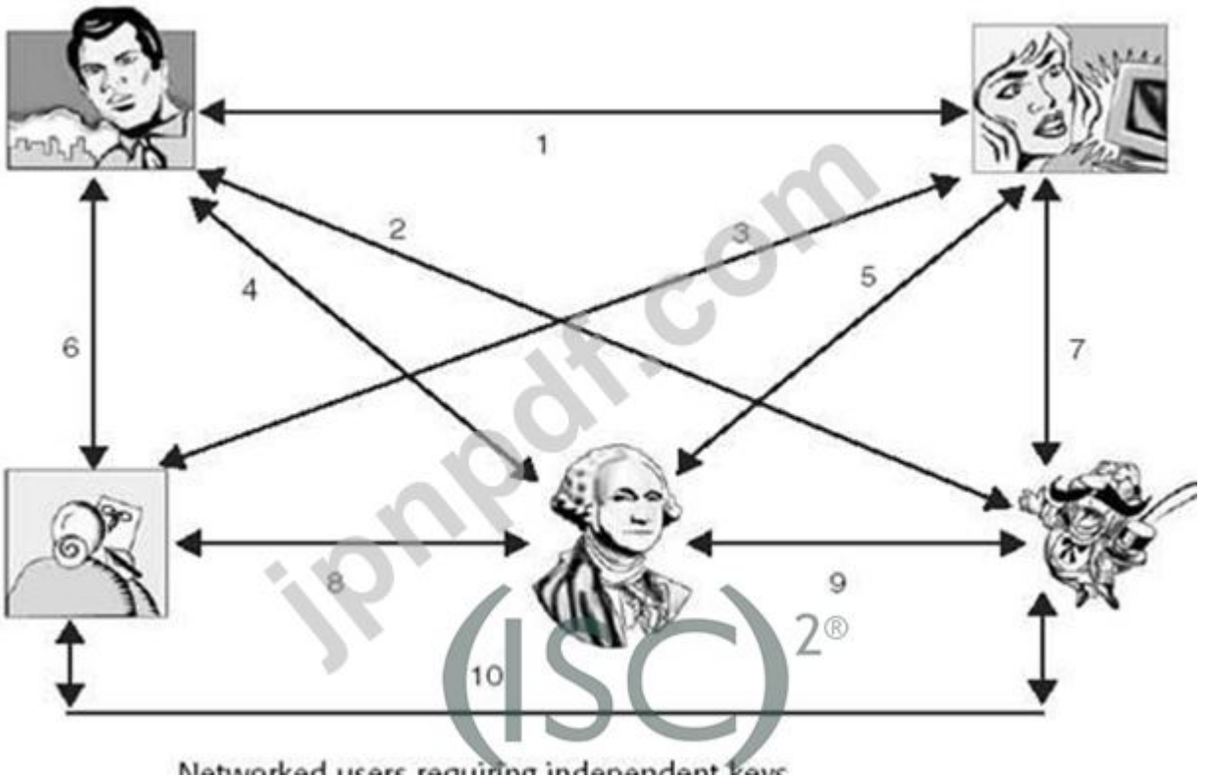


image014
したがって、5人のユーザーの場合、独立したキーの数は 5 x
4）図A.6の10本の接続線で示されているように/2または10。
*回答 「キーの安全な配布」は正しくありません。すべてのユーザーにキーを安全に配布することは、明らかに非常に重要な要件だからです。
キーの妥協は確かに可能性があるため、回答dは正しくありません。
攻撃者がキーの所有者になりすますことができるようにします。
誤ったメッセージを読んで送信します。

最新問題: **391**
スパニングツリープロトコルを定義するIEEEプロトコルはどれですか？
A. IEEE 802.1D
B. IEEE 802.11
C. IEEE 802.5
D. IEEE 802.3
Answer: A (メーッセージを残す**)**
802.1Dスパニングツリープロトコルはイーサネットリンク管理です
ルーティングを防ぎながらリンクの冗長性を提供するプロトコル
ループします。イーサネットネットワークには1つのアクティブパスしか存在できないため、
適切にルーティングすると、STPアルゴリズムが最適なものを計算して管理します
ネットワークを通るループのないパス。
IEEE 802.5は、LANのトークンパッシングリングアクセス方式を指定しています。
IEEE 802.3は、CarrierSenseMultipleを使用してイーサネットバストポロジを指定します
アクセス制御/キャリア検出（CSMA / CD）。

IEEE 802.11は、1Mbpsおよび2Mbpsのワイヤレス接続を指定するIEEE標準です。
2.4 MHz ISM（産業、科学、医療）帯域
出典：MerikeKaeoによるDesigningNetwork Security（Cisco Press、1999）。

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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**: 392**
Open Web Application Security Project（OWASP）過去数年間のリスクのトップ10リスト。
以下のアイテムは長年リストに載っています。以下の選択肢のうち、何年もの間リストの一番上にあった脅威を表すものはどれですか？
A. クロスサイトスクリプティングと動的Unicodeインジェクション攻撃
B. SQLインジェクションおよびクロスサイトスクリプティング攻撃
C. SQLインジェクションと弱い認証およびセッション管理攻撃
D. クロスサイトスクリプティングとセキュリティ設定ミスの攻撃
Answer: (解答を表示する**)**
説明/参照：
Explanation:
SQLインジェクションとクロスサイトスクリプティング攻撃は、OWASPリストの上位2つのリスクです。
2013年の時点でOpenWebApplication Security Project（OWASP）グループによって特定された主なリスクは次のとおりです。
A1：注射
SQL、OS、LDAPインジェクションなどのインジェクションの欠陥は、信頼できないデータがコマンドまたはクエリの一部としてインタープリターに送信されるときに発生します。
A2：クロスサイトスクリプティング（XSS）
A3：壊れた認証とセッション管理
A4：安全でない直接オブジェクト参照
A5：クロスサイトリクエストフォージェリ（CSRF）
A6：セキュリティの設定ミス
A7：安全でない暗号化ストレージ
A8：URLアクセスの制限に失敗しました
A9：不十分なトランスポート層保護

A10：未検証のリダイレクトと転送

不正解：
A :OWASPは、動的Unicodeインジェクションではなく、SQL、OS、およびLDAPインジェクションを指します。
C：弱い認証とセッション管理の攻撃は、OWASPリストで3番目にランク付けされています。
D :セキュリティの設定ミスはOWASPリストで3番目にランク付けされています。
参照：
コンラッド、エリック、セスミゼナル、ジョシュアフェルドマン、CISSP学習ガイド、第2版、Syngress、ウォルサム、
2012年、1109〜1110 ページ

最新問題: **393**
継続的な情報セキュリティ監視プログラムは、次のうちどれを介してリスクを最もよく減らすことができますか？
A. スケジュールされたシステム変更とスケジュールされていないシステム変更の両方をログに記録する
B. セキュリティイベントを収集し、それらを相互に関連付けて異常を特定します
C. 重要なユーザーアカウントのアクティビティに対するシステム全体の可視性を促進します
D. 人、プロセス、テクノロジーを網羅する
Answer: (解答を表示する**)**

最新問題: **394**
次のRAIDレベルのうち、実際には使用されておらず、より柔軟なレベルにすぐに取って代わられたのはどれですか？
A. RAIDレベル0
B. RAIDレベル1
C. RAIDレベル2
D. RAIDレベル7
Answer: C (メーッセージを残す**)**
RAIDレベル2が正解です。RAIDレベル2は実際には使用されておらず、
より柔軟なレベルにすぐに取って代わられました。出典 :KRUTZ、Ronald L.＆VINES、Russel D.、CISSP準備ガイド :コンピュータセキュリティの10のドメインをマスターする、2003年、John Wiley＆
息子、90ページ。
RAIDレベル1"このレベルは、あるディスクから別のディスクへのすべてのディスク書き込みを複製して、2つの同一のディスクを作成します
ドライブ。この手法は、データミラーリングとも呼ばれます。このレベルでは冗長性が提供されます。いつ

1台のハードドライブに障害が発生しても、もう1台は引き続き使用できます。ミラーリングにより、ハードドライブの冗長性も可能になります
コントローラー。これは二重化と呼ばれます。」出典：CISSPCBKの公式ISC2ガイドp。657
RAIDレベル0"パリティ情報を使用せずに、複数のディスクにまたがってファイルをストライプで書き込みます。
この手法により、ディスクの読み取りと書き込みを高速化できます。ただし、パリティ情報がないと、
ハードドライブの障害から回復することはできません。この手法は冗長性を提供しません
また、高可用性要件のあるシステムには使用しないでください。"出典：公式ISC2
CISSPCBKのガイドp。657
RAIDレベル7-非標準RAIDレベル。非標準RAIDレベルについては、ウィキペディアの記事を参照してください。

最新問題: **395**
システム高セキュリティモードと専用セキュリティモードの最大の違いは次のとおりです。
A. 必要なクリアランス
B. オブジェクト分類
C. 被験者はすべてのオブジェクトにアクセスできません
D. 知っておくべきこと
Answer: D (メーッセージを残す**)**
「知る必要がある」は正しいです。専用セキュリティモードでは、対象者は
システムに含まれるすべての情報について「知る必要がある」。システム高の場合
セキュリティモード対象者は、アクセスしようとしている情報についてのみ「知る必要がある」必要があります。
次の答えは正しくありません。
「必要なクリアランス」
システム上のすべてのデータに同じクリアランスが必要なため、これは正しくありませんが、これは両方のシステムで同じです。
「オブジェクト分類」
システム上のすべてのデータが同じ分類レベルを必要とするため、これは正しくありません。
知る必要があるのはオブジェクトのラベルの一部ですが、これは最良の答えではありません。
「被験者はすべてのオブジェクトにアクセスできない」
より正しい答えを知る必要があるため、これは正しくありません。知る必要があるため、特定のサブジェクトはすべてのオブジェクトにアクセスできるわけではありませんが、最良の答えは知る必要があります。
この質問を作成するために、次の参照が使用されました。
ISC2OIGp.841およびp.995
ションハリスAIO、第4版、p。297
http://www.fas.org/irp/nsa/rainbow/tg004.htm

最新問題: **396**
次のうち、最もセキュリティの問題の原因となっているのはどれですか？
A. スパイの外
B. ハッカー
C. 人員
D. 機器の故障
Answer: (解答を表示する**)**
コメントで先に述べたように、企業への攻撃の大部分は人員によるものです。ハッカーはそこにいて、いくつかのターゲットを攻撃しますが、最悪の敵があなたの会社の中にいる可能性があることを決して忘れてはなりません。そのために、私たちは通常IDSと深遠なセキュリティを実装しています。ホストベースのIDSをインストールして、マシンを介した内部攻撃者の能力を制限することは非常に良い習慣です。
個人に関するもう1つの問題は、無知です。彼らが何をしているのかわからず、確かにセキュリティポリシーに違反している場合があります。

最新問題: **397**
Bell-LaPadulaセキュリティモデルに関連する次のステートメントのどれが間違っていますか $trong Starプロパティが使用されていないことを前提としています）？
A. 件名は読み上げできません。
B. *-プロパティの制限は、高レベルのサブジェクトを一時的にダウングレードすることで回避できます。
C. 被験者は読み下ろすことができません。
D. 機密保持に制限されています。
Answer: (解答を表示する**)**
ベルラパドゥラモデルの所有物ではありません。
他の答えは正しくありません：
主題は読むことを許可されていませんベルラパドゥラの 単純なセキュリティルール」のプロパティです
モデル。
*-プロパティの制限は、高レベルのサブジェクトを一時的にダウングレードすることで回避できます。
高レベルのサブジェクトを一時的にダウングレードするか、信頼できるオブジェクトのセットを識別することによって回避されました
操作の途中でない限り、*プロパティに違反することが許可されます。
機密性を強制するステートマシンモデルであるため、機密性に制限されます
アクセス制御の側面。
参照 :ションハリスAIO v3、第5章 :セキュリティモデルとアーキテクチャ、ページ :279-282

最新問題: **398**

セキュリティの観点から、ドメインネームサービス（DNS）システムを構成するためのベストプラクティスは次のうちどれですか？
A. すべての伝送制御プロトコル（TCP）接続をブロックする
B. 許可されたデバイスへのゾーン転送を制限する
C. ネームサーバーでのすべての再帰クエリを無効にします
D. プライマリサーバーをゾーンフォワーダーとして使用するようにセカンダリサーバーを構成します
Answer: (解答を表示する**)**

最新問題**: 399**
US-EUセーフハーバープロセスは、次のうちどれに対処するために作成されましたか？
A. 米国とヨーロッパの企業間で転送されるデータの整合性
B. 米国とヨーロッパの企業間で転送されるデータの機密性
C. 米国とヨーロッパの企業間で転送される個人データの保護
D. ヨーロッパ企業と国際企業間で転送されるデータの機密性
Answer: C (メーッセージを残す**)**
US-EUセーフハーバーは、米国企業が個人データの保護に関するEU指令95/46/ECに準拠するための合理化されたプロセスです。
欧州委員会のデータ保護に関する指令は1998年10月に発効し、欧州連合以外の国への個人データの転送を禁止します。
プライバシー保護のための欧州連合（EU）の「妥当性」基準。
米国とEUは、プライバシー保護を強化するという目標を共有しています。
市民である米国は、EUが採用しているものとは異なるプライバシーへのアプローチを採用しています。順番に
これらのアプローチの違いを埋め、米国の組織が
欧州と協議して米国商務省の指令に準拠する
委員会は、情報を提供するための「セーフハーバー」フレームワークとウェブサイトを開発しました。
組織は、US-EUセーフハーバープログラムを評価し、次に参加する必要があります。リンクを見る下記のウェブサイトへ。
顧客データを保存するEUまたは米国内の組織を対象としたセーフハーバー
原則は、偶発的な情報の開示または損失を防ぐように設計されています。米国企業は
指令で概説されている7つの原則に準拠している限り、プログラムにオプトインします。
これらの原則は以下を提供する必要があります。
通知個人は、データが収集されていることと、そのデータがどのようになるかについて通知を受ける必要があります
使用済み。
選択個人は、収集をオプトアウトし、転送を転送する機能を持っている必要があります
第三者へのデータ。
転送サードパーティへのデータの転送は、他の組織にのみ発生する可能性があります

適切なデータ保護の原則に従ってください。
セキュリティ収集した情報の損失を防ぐために、合理的な努力を払う必要があります。
データの整合性データは、収集された目的に関連し、信頼できるものでなければなりません。
アクセス個人は、自分について保持されている情報にアクセスし、次の場合にそれを修正または削除できる必要があります
不正確です。
施行これらの規則を施行する効果的な手段がなければなりません。
このプロセスは、米国商務省がEUと協議して開発したものです。
次の答えは正しくありません。
米国とヨーロッパの企業間で転送されるデータの整合性：整合性は目標ではありません
セーフハーバーの要件。
米国とヨーロッパの企業間で転送されるデータの機密性：機密性は
セーフハーバー要件の目標
欧州企業と国際企業の間で転送されるデータの機密性：セーフハーバーには
米国企業と取引するために作成されており、機密保持に重点を置いていません。
この質問を作成するために、次の参照が使用されました。
オールインワンbyションハリス第5版p 855）
ウィキペディア：米国商務省は、セーフハーバーと呼ばれる認証プログラムを実行しており、米国と欧州連合指令95/46/ECとの間の取引におけるデータプライバシー慣行を調和させることを目的としています。個人データの保護。詳細については、セーフハーバーの原則を参照してください。http://export.gov/safeharbor/eu/eg_main_018365.asp：米国欧州連合セーフハーバー

最新問題: **400**
TCPとUDPの違いについて正しい答えは次のうちどれですか？
A. UDPはコネクションレス型プロトコルと見なされ、TCPはコネクション型です。
B. TCPはコネクションレス型プロトコルと見なされ、UDPはコネクション型です。
C. TCPは、信頼性の低いプロトコルと呼ばれることもあります。
D. UDPはパケットの受信を確認しますが、TCPは確認しません。
Answer: A (メーッセージを残す**)**
正解は「UDPはコネクションレス型プロトコルと見なされ、TCPはコネクション型です」です。伝送制御プロトコル（TCP）とは対照的に、ユーザー
データグラムプロトコル（UDP）はコネクションレス型です
プロトコル。パケットをシーケンスせず、確認します
パケットの受信であり、信頼性の低いプロトコルと呼ばれます。

最新問題: **401**
このOSI層には、転送構文をネゴシエートし、ユーザーの転送構文との間でデータを変換するサービスがあります。これは、さまざまな構文を使用してデータを表す場合があります。次のどのレイヤーでそのようなサービスを見つけますか？
A. セッション

B. 輸送
C. プレゼンテーション
D. アプリケーション
Answer: C (メーッセージを残す**)**
「アプリケーション層プロトコル」から情報を取得し、アプリケーションが処理するのに適した形式にする責任があります。
OSIプロトコルスイートのプレゼンテーション層の実装は、プレゼンテーションプロトコルとプレゼンテーションサービスで構成されています。プレゼンテーションプロトコルにより、プレゼンテーションサービスユーザー（PSusers）はプレゼンテーションサービスと通信できます。
PSユーザーは、プレゼンテーション層のサービスを要求するエンティティです。このような要求は、プレゼンテーションサービスアクセスポイント（PSAP）で行われます。PSユーザーは、PSAPアドレスを使用して一意に識別されます。
プレゼンテーションサービスは、転送構文をネゴシエートし、転送構文との間でデータを変換します
さまざまな構文を使用してデータを表すPSユーザー向け。プレゼンテーションサービスは
使用される転送構文に同意する2人のPSユーザー。転送構文が合意されたとき
その際、プレゼンテーションサービスエンティティは、PSユーザーからのデータを正しい転送に変換する必要があります
構文。
OSIプレゼンテーション層サービスは、ISO8822標準およびITU-TX.216で定義されています。
おすすめ。OSIプレゼンテーションプロトコルは、ISO8823標準および
ITU-TX.226の推奨事項。プレゼンテーションプロトコルのコネクションレスバージョンは、ISO9576規格。
OSI層を覚えておくために、次のニーモニックを使用できます。
最初のものは下から（物理層-レイヤー1）上（アプリケーション-レイヤー7）です：
ソーセージピザを捨てないでください
上から下に別のニーモニックがあります。
すべての人がデータ処理を必要としているようです
両方のマップ：
1.物理-2.データリンク-3.ネットワーク-4.トランスポート-5.セッション-6.プレゼンテーション-7.アプリケーション
次の回答は正しくありません。トランスポート :エンドツーエンドのデータトランスポートサービスを提供し、TCPやUDPなどのコンピュータ間の論理接続を確立する責任があります。
セッション :データ転送中に2つのアプリケーション間の接続を維持する責任があります。たとえばNFS、RPCプロトコルアプリケーション :アプリケーションに最も近く動作します。アプリケーション自体は含まれていませんが、アプリケーションをサポートするプロトコルが含まれています。たとえば、HTTPはこのレイヤーで機能しますが、サポートするアプリケーションは
IE、Mozilla、opera、chrome..です。

この質問を作成するために、次の参照が使用されました：
http://www.cisco.com/cpress/cc/td/cpress/fund/ith2nd/it2432.htmおよびhttp://en.wikipedia.org / wiki / List_of_network_protocols_%28OSI_model%29

最新問題: **402**
アナリストがいくつかの平文と暗号文のペアの知識から鍵を決定しようとする暗号解読技術として最もよく定義できるのは、次のうちどれですか？
A. 既知平文攻撃
B. 既知のアルゴリズムによる攻撃
C. 選択暗号文攻撃
D. 選択平文攻撃
Answer: A (メーッセージを残す**)**
RFC2828（Internet Security Glossary）は、既知平文攻撃を暗号解読技術として定義しています。この技術では、アナリストは、いくつかの平文と暗号文のペアの知識からキーを決定しようとします ただし、アナリストは、暗号アルゴリズムを知るなど、他の手がかりを持っている場合もあります）。）。選択暗号文攻撃は、分析者がに対応する平文の知識から鍵を決定しようとする暗号解読技術として定義されます。
アナリストによって選択された（つまり、口述された）暗号文。選択平文攻撃は暗号解読です
アナリストが暗号文の知識からキーを決定しようとする手法
アナリストが選択した（つまり、口述した）平文に対応します。他の選択肢は気を散らすものです。以下は不正解です。
選択平文攻撃
攻撃者は平文と暗号文を持っていますが、暗号化される平文を選択できます
対応する暗号文を参照してください。これは彼女により多くの力とおそらくより深い理解を与えます
暗号化プロセスが機能する方法について、彼女はキーが存在することについてより多くの情報を収集できるようになります
使用済み。キーが検出されると、そのキーで暗号化された他のメッセージを復号化できます。
選択暗号文攻撃
選択暗号文攻撃では、攻撃者は復号化する暗号文を選択でき、
結果の復号化された平文へのアクセス。繰り返しますが、目標は鍵を理解することです。これは難しいです
前述の攻撃と比較して実行する攻撃、および攻撃者はする必要があるかもしれません
暗号システムを含むシステムを制御できます。
既知のアルゴリズム攻撃
アルゴリズムを知っていても、鍵を知らなくてもあまり利点はありません。これは
偽の批判者。アルゴリズムは公開されている必要があります。これはケルクホフスの原理です。唯一の
秘密が鍵となるはずです。
この質問に使用される参照：

出典：SHIREY、Robert W.、RFC2828：Internet Security Glossary、2000年5月。
と
ハリス、ショーン（2012-10-25）。CISSPオールインワン試験ガイド、第6版（p.866）。マグロウヒル。キンドル版。
と
ケルクホフスの原理

最新問題: **403**
平文の各ビットまたは文字がモジュール式の追加によって暗号化されるメッセージと同じ長さのキーを使用するものは何ですか？
A. 実行中のキー暗号
B. ワンタイムパッド
C. ステガノグラフィ
D. 暗号ブロック連鎖
Answer: (解答を表示する**)**
暗号化では、ワンタイムパッド（OTP）は、正しく使用された場合に解読できない暗号化の一種です。平文の各ビットまたは文字は、平文と同じ長さの秘密のランダムキー（またはパッド）からのビットまたは文字をモジュール式に追加することによって暗号化され、暗号文になります。キーが本当にランダムであり、少なくとも平文であり、全体または一部が再利用されることはなく、秘密にされている場合、暗号文はキーを知らずに復号化または解読することはできません。また、完全な機密性を備えた暗号は、OTPキーと実質的に同じ要件のキーを使用する必要があることも証明されています。しかし、実際の問題により、ワンタイムパッドを広く使用することはできませんでした。
1882年にフランクミラーによって最初に記述されたワンタイムパッドは、1917年に再発明され、数年後に特許を取得しました。これは、発明者の1人であるGilbertVernamにちなんで名付けられたVernam暗号から派生しています。バーナムのシステムは、メッセージとから読み取られたキーを組み合わせた暗号でした。
パンチテープ。元の形式では、キーテープが
ループ。ループが完全なサイクルになるたびに再利用されました。1回限りの使用は少し遅れて来ました
ジョセフ・モーボルグネが、キーテープが完全にランダムである場合、暗号解読は
不可能であること。
名前の「パッド」の部分は、主要な材料があった初期の実装に由来します
紙のパッドとして配布されるため、使用後にトップシートが簡単に剥がれて破壊される可能性があります。為に
簡単に隠すことができ、パッドは時々非常に小さいサイズに縮小されたため、強力です
使用するには虫眼鏡が必要でした。写真は、手のひらに収まるキャプチャされたKGBパッドを示しています
自分の手、またはクルミの殻の中。セキュリティを強化するために、ワンタイムパッドが印刷されることがありました

可燃性の高いニトロセルロースのシートで、すぐに燃やすことができます。
以下は不正解です。
実行中のキー暗号は、電子アルゴリズムではなく、物理的な世界の記事を使用します。の
古典的な暗号化では、実行中の鍵暗号は、多表式暗号の一種です。
これは、通常は本からのテキストであり、非常に長いキーストリームを提供するために使用されます。通常、本は
使用する通路は事前に合意され、使用する通路はランダムに選択されます
各メッセージとメッセージのどこかに密かに示されています。
ランニングキー暗号は、ヴィジュネル暗号と同じ内部動作をします。違い
キーの選択方法にあります。ヴィジュネル暗号は繰り返される短い鍵を使用しますが、
実行中のキー暗号は、本からの抜粋などの長いキーを使用します。これは、キーが
繰り返して、暗号解読をより困難にします。ただし、暗号はまだ破られている可能性があります。
悪用される可能性のあるキーとプレーンテキストの両方の統計パターン。
ステガノグラフィは、メッセージの存在そのものを隠す方法です。それは芸術です
送信者と送信者を除いて誰もいないような方法で隠されたメッセージをエンコードする科学
意図された受信者は、メッセージの存在を疑っています。隠れることと呼ばれることもあります
プレーンサイト。
暗号ブロック連鎖はDES動作モードです。IBMは暗号ブロック連鎖（CBC）を発明しました
1976年の動作モード。CBCモードでは、平文の各ブロックは前のブロックとXORされます。
暗号化される前の暗号文ブロック。このように、各暗号文ブロックはすべての平文に依存します
その時点までに処理されたブロック。各メッセージを一意にするには、初期化ベクトルは次のようにする必要があります
最初のブロックで使用されます。
この質問に使用される参照：
HARRIS、ション、オールインワンCISSP認定試験ガイド、McGraw-Hill / Osborne、2002年、章8：暗号化555ページ）。およびhttp://en.wikipedia.org/wiki/One-time_pad
http://en.wikipedia.org/wiki/Running_key_cipher
http://en.wikipedia.org/wiki/Cipher_block_chaining#Cipher-block_chaining_.28CBC.29

最新問題: **404**
従来のWebアプリケーションのセキュリティ問題に対処するための最良のアプローチは何ですか？
A. セキュリティ評価を実施する
B. 可能な場合は、サポートされている新しいアプリケーションに移行します
C. セキュリティの問題をデバッグする
D. Webアプリケーションファイアウォールでレガシーアプリケーションを保護する
Answer: (解答を表示する**)**

最新問題: **405**

テレフォニーでは、さまざまなタイプの接続が使用されています。電話会社の支店から地元の顧客への接続は、次の選択肢のどれと呼ばれますか？
A. 新しいループ
B. ローカルループ
C. ループバック
D. 固有のループ
Answer: B (メーッセージを残す**)**
説明/参照：
Explanation:
テレフォニーでは、ローカルループは、顧客宅内の境界点から通信事業者または電気通信サービスプロバイダーのネットワークのエッジに接続する物理的なリンクまたは回線です。
不正解：
A：新しいループは一種の接続ではありません。
C：ループバックインターフェイスは、シリアル通信トランシーバーがその機能をテストするためにループバックを使用できることです。
D：固有のループは一種の接続ではありません。
参照：
https://en.wikipedia.org/wiki/Local_loop

最新問題**: 406**
事業継続計画（BCP）をテストするためのベストプラクティスは次のうちどれですか？
A. セキュリティパッチのインストール後にテストする
B. システムパッチの実装後にテストする
C. 環境が変化したときにテストする
D. IT監査の前にテストする
Answer: C (メーッセージを残す**)**

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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**: 407**
「システム整合性」とはどういう意味ですか？
A. システムのソフトウェアは設計どおりに実装されています。
B. ユーザーは自分が所有していないプロセスを改ざんすることはできません。

C. ハードウェアとファームウェアは、正しく機能していることを確認するために定期的なテストを受けています。
D. 設計仕様は、正式なトップレベルの仕様に対して検証されています。
Answer: C (メーッセージを残す**)**
説明/参照：
Explanation:
システムの整合性とは、システムのすべてのコンポーネントが権限のない担当者によって改ざんされることがなく、正しく機能していることを確認できることを意味します。
不正解：
A :システム整合性は、ソフトウェアの実行方法に関係し、ソフトウェアの実装には関係しません。
C :システム整合性は、ハードウェアとファームウェアの検証を意味するものではありません。システム整合性は、実行中のソフトウェアの動作に関連しています。
D :システム整合性は仕様検証の一部ではありません。システム整合性は、ソフトウェアの実行方法に関係します。
参照：
http://www.cerberussystems.com/INFOSEC/stds/d520028.htm
コンラッド、エリック、セスミゼナル、ジョシュアフェルドマン、CISSP学習ガイド、第2版、Syngress、ウォルサム、
2012年、p。12

最新問題**: 408**
セキュリティ意識向上プログラムの目的は、以下を改善することです。
A. ベンダー関係のセキュリティ。
B. データの保護に関する会社の姿勢。
C. 企業のイントラネットのパフォーマンス。
D. ITスタッフのキャリアアップの可能性。
Answer: B (メーッセージを残す**)**

最新問題**: 409**
通常はログオンIDの形式で、システムにIDを公言するユーザーの行為とは何ですか？
A. 認証
B. 識別
C. 承認
D. 守秘義務
Answer: B (メーッセージを残す**)**
説明/参照：
Explanation:
識別には、ユーザーがユーザー名、ユーザーID、またはアカウント番号を使用して識別情報を提供することが含まれます。
不正解：

A：認証には、パスフレーズ、PIN値、生体認証、ワンタイムパスワード、またはパスワードを使用してユーザーの識別情報を確認することが含まれます。
C：承認とは、ユーザーが特定のリソースへのアクセスを許可されているかどうか、およびそのリソースに対して実行が許可されているアクションをシステムが確立することです。
D：機密性は、データ処理のすべての接合部に必要なレベルの機密性が課され、不正な開示を防止するために使用されます。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、2013、pp.24、166、203

最新問題: **410**
一般に、インターネットに面しているサーバーは、非武装地帯（DMZ）に配置する必要があります。DMZの主な目的は何ですか？
A. 公開されたサーバーに関連するリスクを軽減します。
B. 内部システムへのリスクを軽減します。
C. ファイアウォールの必要性を回避します。
D. 潜在的な攻撃に備えてサーバーを準備します。
Answer: B (メーッセージを残す**)**

最新問題: **411**
システムログを6か月以上保持することは、どのような活動に役立つ可能性がありますか？
A. IDおよび承認の管理
B. フォレンジックとインシデント対応
C. 物理的および論理的なアクセス制御
D. ディザスタリカバリとビジネス継続性
Answer: B (メーッセージを残す**)**

最新問題: **412**
ただし、雇用主が後援または維持しているグループ健康保険
A. カバーされていないエンティティと呼ばれます
B. 時々対象となるエンティティです。
C. 対象となるエンティティ
D. 対象となるエンティティではありません。
Answer: C (メーッセージを残す**)**

最新問題: **413**
ソフトウェア製品の品質が、関連するソフトウェア開発および保守プロセスの品質の直接的な関数であるという前提に基づいて、ソフトウェアプロセスに関与する組織の成熟度を評価する5つのレベルを導入したモデルはどれですか。
A. 総合的品質モデル（TQM）
B. 理想的なモデル

C. ソフトウェア機能成熟度モデル
D. スパイラルモデル
Answer: (解答を表示する**)**
説明/参照：
Explanation:
Software Capability Maturity Model（CMM）は、ソフトウェア製品の品質が、関連するソフトウェア開発および保守プロセスの品質の直接的な関数であるという前提に基づいています。継続的なプロセス改善を実施するための基盤として、またソフトウェアプロセスに関与する組織の成熟度を測定するための順序尺度として機能する5つの成熟度レベルを紹介します。
CMMには、ソフトウェアプロセスの5つの成熟度レベルがあります。
初期レベル :プロセスはまとまりがなく、混沌としている。成功は個人に依存する可能性があります
▪
プロセスは十分に定義および文書化されていないため、複製できるとは見なされません。
反復可能または管理されたレベル：基本的なプロジェクト管理手法が確立され、
▪
必要なプロセスが確立され、定義され、文書化されているため、成功を繰り返すことができます。
定義されたレベル：組織は、より優れた方法で独自の標準ソフトウェアプロセスを開発しました
▪
ドキュメント、標準化、および統合への注意。
定量的に管理されるレベル：組織は、データを通じて独自のプロセスを監視および制御します
▪
収集と分析。
最適化されたレベル :プロセスは、からのフィードバックを監視することで常に改善されています
▪
現在のプロセスと、組織の特定のニーズにより適切に対応するための革新的なプロセスの導入。
不正解：
A：総合品質管理（TQM）は、すべてのメンバーの参加に基づいて、顧客満足を通じて長期的な成功を目指す、品質を中心とした組織の管理アプローチです。
B：負荷の統合設計、評価、および評価（IDEAL）モデルは、雨水に関する最良の管理手法を設計するための建設後の水質モデルです。ソフトウェア開発モデルではありません。
D :スパイラルモデルは、リスク分析に重点を置いたソフトウェア開発への反復アプローチを使用しています。反復的なアプローチにより、新しい要件が明らかになったときに対処することができます。これは、流動的な要件がある複雑なプロジェクトに適したモデルです。
スパイラルモデルには、次の4つの主要なフェーズがあります。
計画
▪
リスク分析 :すべての問題が積極的にレビューおよび分析されるようにします。
▪
開発とテスト :プロトタイプテストは開発プロジェクトの早い段階で行われ、フィードバックがあります
▪
これらのテストに基づいて、次のステップの反復に統合されます。
評価：顧客は現在の状態で製品を評価し、フィードバックを提供します。これは
▪
次のステップの反復の入力値。

参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、New York、2013、pp。62、1115-1116、1120-1122
http://en.wikipedia.org/wiki/Capability_Maturity_Model
https://en.wikipedia.org/wiki/Total_quality_management
https://en.wikipedia.org/wiki/IDEAL_model

最新問題**: 414**
適切な構成プロセスの重要な要素に関するこれらの記述のうち、正しくないものはどれですか？
A. 実証済みの標準とベストプラクティスの再利用に対応
B. すべての要件が明確、簡潔、有効であることを確認します
C. リソースの変更を防ぐために、システムハードウェアの変更を制御します
D. 変更、標準、および要件が迅速かつ正確に伝達されるようにします
Answer: C (メーッセージを残す**)**
説明/参照：
Explanation:
標準は、適切な構成管理プロセスと承認されたベースライン構成設定の概要を示すために開発されています。システムは、標準に規定されているものに対してテストでき、システムを監視して、標準に概説されている要件を満たさない構成があるかどうかを検出できます。
優れた構成プロセスは、実証済みの標準とベストプラクティスに従います。要件は、明確、簡潔、かつ有効である必要があります。変更、標準、および要件は、迅速かつ正確に伝達する必要があります。
『リソースの変更を防ぐためにシステムハードウェアの変更を制御する」というステートメントは、適切な構成プロセスの重要な要素ではありません。システムハードウェアへの変更は、変更管理手順によって制御する必要があります。
不正解：
A：実績のある標準とベストプラクティスの再利用に対応することは、優れた構成プロセスの重要な要素の1つです。
B :すべての要件が明確、簡潔、有効であり続けることを保証することは、優れた構成プロセスの重要な要素の1つです。
D：変更、標準、および要件が迅速かつ正確に伝達されるようにすることは、優れた構成プロセスの重要な要素の1つです。

最新問題**: 415**
次のうち、侵入テストを実行するために使用される手法ではないものはどれですか？
A. トラフィックパディング
B. スキャンとプロービング
C. 戦争ダイヤリング
D. スニッフィング

Answer: A (メーッセージを残す**)**
トラフィックパディングは、トラフィック分析の対策です。
完全な暗号化ルーチンが使用されている場合でも、攻撃者は生成されたトラフィックの量を知ることができます。攻撃者は、アリスとボブが何について話しているのかを知らないかもしれませんが、彼らが話していることと、彼らがどれだけ話しているかは知ることができます。特定の状況では、これは非常に悪い場合があります。たとえば、軍隊が他国に対する秘密攻撃を組織している場合を考えてみてください。他国に、多くの秘密活動が行われていることを単に知ってもらうように警告するだけで十分かもしれません。
別の例として、可変ビットレートエンコーディングを使用するVoice Over IPストリームを暗号化する場合、単位時間あたりのビット数が不明瞭になることはなく、これを利用して話し言葉を推測することができます。
メッセージのパディングは、トラフィック分析を困難にする方法です。通常、メッセージの最後にいくつかのランダムビットが追加され、最後にこのランダムデータの量が示されます。ランダム性は、最小値が0、最大数がNで、2つの極値の間で均等に分布している必要があります。0を増やしても効果はなく、Nを増やすだけで効果がありますが、実際のデータの送信に使用されるチャネルの割合が低くなることも意味します。また、暗号化ルーチンはクラックできないと想定されているため そうでない場合、パディングの長さ自体はクラック可能です)、パディングを他の場所、たとえば最初、途中、または散発的に配置することは役に立ちません。他の答えは、侵入テストを行うために使用されるすべての技術です。
参考資料 :KRUTZ、Ronald L.＆VINES、Russel D.、CISSP Prep Guide :Mastering the Ten Domains of Computer Security、233、238ページ。および
https://secure.wikimedia.org/wikipedia/en/wiki/Padding_ %28cryptography%29＃Traffic_analysis

最新問題**: 416**
セキュリティアーキテクトは、実装のために強制アクセス制御 MAC)モデルを参照することを計画しています。これは、次のプロパティのどれが優先されているかを示していますか？
A. 守秘義務
B. 整合性
C. 可用性
D. アクセシビリティ
Answer: A (メーッセージを残す**)**
セクション :ソフトウェア開発のセキュリティ
Explanation:
強制アクセス制御 MAC)は、サブジェクトのクリアランスとオブジェクトのラベルに基づくシステム強制アクセス制御です。サブジェクトとオブジェクトには、それぞれ、機密、秘密、極秘などのクリアランスとラベルがあります。サブジェクトは、サブジェクトのクリアランスがオブジェクトのラベル以上である場合にのみ、オブジェクトにアクセスできます。サブジェクトは、適切なクリアランスがない他のサブジェクトとオブジェクトを共有したり、オブジェクトをより低い分類

レベル（極秘から秘密など）に 書き留め」たりすることはできません。MACシステムは通常、データの機密性を維持することに重点を置いています。
参照 :https ://www.sciencedirect.com/topics/computer-science/mandatory-access-control

最新問題: **417**
情報の許可された転送のために設計されたコンピュータシステムまたはネットワーク内のチャネルは、a ｎ）として識別されますか？
A. 被覆通信路
B. 明白なチャネル
C. 開いたチャンネル
D. 閉じたチャネル
Answer: (解答を表示する**)**
明白なチャネルは、データの許可された転送のために設計されたコンピュータシステムまたはネットワーク内のパスです。反対は、許可されていないパスである秘密チャネルです。
秘密チャネルは、エンティティが不正な方法で情報を受信するための方法です。これは、セキュリティメカニズムによって制御されない情報フローです。このタイプの情報パスは、通信用に開発されたものではありません。したがって、開発者は情報がこのように渡されることを想定していなかったため、システムはこのパスを適切に保護しません。この方法で情報を受信すると、明らかにシステムのセキュリティポリシーに違反します。
他のすべての選択肢は偽の批判者です。
この質問に使用される参照：
KRUTZ、Ronald L.＆VINES、Russel D.、CISSP準備ガイド :10をマスターする
Domains of Computer Security、2001年、John Wiley＆Sons、219ページ。
と
ション ハリス、CISSPオールインワン AIO）、第6版、380ページ
と
ハリス、ション 2012-10-25）。CISSPオールインワン試験ガイド、第6版 ｐ.378）。マグロウ-丘。キンドル版。

最新問題: **418**
次の生体認証特性のうち、個人のIDを一意に認証するために使用できないものはどれですか？
A. パームスキャン
B. 網膜スキャン
C. 皮膚スキャン
D. 虹彩スキャン
Answer: C (メーッセージを残す**)**

最新問題: **419**
相互認証の主な役割は何ですか？
A. 異なるPKI間の信頼の作成

B. 全体的なPKI階層を構築する
C. 2番目のルートCAへの直接信頼を設定します
D. CA証明書の失効によるユーザー証明書の無効化を防止します
Answer: A (メーッセージを残す**)**
ますます多くの組織が独自の内部PKIを設定しています。これらの独立したPKIが相互接続して（部門間または異なる会社間で）安全な通信を行えるようにする必要がある場合、2つのルートCAが相互に信頼する方法が必要です。
これらの2つのCAには、両方が信頼できるCAが上にないため、相互認証を実行する必要があります。相互認証とは、CAが信頼関係を確立するために行うプロセスであり、CAは、相互のデジタル証明書と公開鍵を、自分で発行したかのように信頼します。
これを設定すると、ある会社のCAが他の会社のデジタル証明書を検証したり、その逆を行ったりすることができます。
この質問に使用される参照：
相互認証の詳細と図については、以下をご覧ください。
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03qswp.mspx http://www.entrust.com/resources/pdf/cross_certification.pdfも参照してください：
ション・ハリス、CISSPオールインワンブック、第4版、727ページ
と
RFC 2459 :インターネットX.509公開鍵インフラストラクチャ証明書およびCRLプロファイル。
フォード、
Warwick＆BAUM、Michael S.、Secure Electronic Commerce：Building the Infrastructure for
デジタル署名と暗号化（第2版）、2000年、Prentice Hall PTR、254ページ。

最新問題**: 420**
Ding Ltd.は、知的財産事業を専門とする会社です。しっかりしたセキュリティプログラムに従って年次意識向上プログラムを実施するために、新しいビデオストリーミングアプリケーションをインストールする必要があります。アプリケーションは、内部で著作権で保護されたコンピューターベースのトレーニングビデオをストリーミングします。アプリケーションのインストールの要件は、単一のサーバー、低コストのテクノロジー、高性能、および高可用性容量を使用しないことです。
ストレージテクノロジーに関して、サーバーのハードドライブに最適な構成は何ですか？
A. 単一のハードディスク（RAIDなし）
B. RAID 0
C. RAID 1
D. RAID 10
Answer: A (メーッセージを残す**)**
単一のハードディスクは、低コストの要件と高可用性を提供しませんが、高性能を提供しません
RAID 1（ミラーリング）は、ニーズの正反対を提供します。低パフォーマンス、高コスト、高可用性
RAID 10はパフォーマンスを提供しますが、高可用性容量を備えた高価なソリューションです。

この質問を作成するために、次の参照が使用されました :ションハリス、AIO 5th、運用セキュリティ、1086ページ

最新問題: **421**
セキュリティを対象とする内部サービスレベル契約（SLA）は、上級管理職によって署名され、実施されています。
優れたセキュリティ体制が提供されていることを確認するために、SLAへの準拠をいつ確認する必要がありますか？
A. 定期的な会議で
B. SLA更新プロセスの一環として
C. 計画されたセキュリティ監査の前
D. セキュリティ違反の直後
Answer: (解答を表示する**)**

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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: **422**
AAAサーバー（Radius、TACACS、DIAMETER）が提供するサービスではないものは次のうちどれですか？
A. 認証
B. 管理
C. 会計
D. 承認
Answer: B (メーッセージを残す**)**
RADIUS、TACACS、およびDIAMETERは、認証、承認、
およびアカウンティング（AAA）サーバー。
出典 :TIPTON、Harold F.&KRAUSE、MICKI、Information Security Management Handbook、4th Edition、Volume 2、2001、CRC Press、NY、33ページ
も参照してください：
「AAA」という用語はよく使用され、[AICトライアドの]基本的な概念を説明します。
承認、および説明責任。AAAの頭字語から除外されているのは、必要なIDです。
3つの「A」が続く前に。アイデンティティは主張であり、認証はアイデンティティを証明し、
承認とは、識別された後にシステムで実行できるアクションのことです。
と認証され、説明責任はユーザーに彼らの行動に対する責任を負わせます。

参照 :CISSP研究ガイド、コンラッドミセナー、フェルドマンp。10-11、©2010エルゼビア。

最新問題: **423**
セキュリティプログラムに必要な機能に次のうちどれが含まれる場合は常に、警備員が適切ですか？
A. 差別的な判断の使用。
B. 物理的な力の使用。
C. アクセス制御デバイスの操作。
D. 不正アクセスを検出する必要があります。
Answer: A (メーッセージを残す**)**
これは正解です。物理的な力を使用するためだけに警備員がいるわけではありません。セキュリティポリシーが適切に設定されている場合、警備員の実際の機能ではありません。CISSPのドキュメントに記載されているように、これらは制御デバイスを操作し、不正アクセスを検出するためだけに存在するのではなく、セキュリティプログラム内のガードの適切な機能は差別的な判断の使用です。

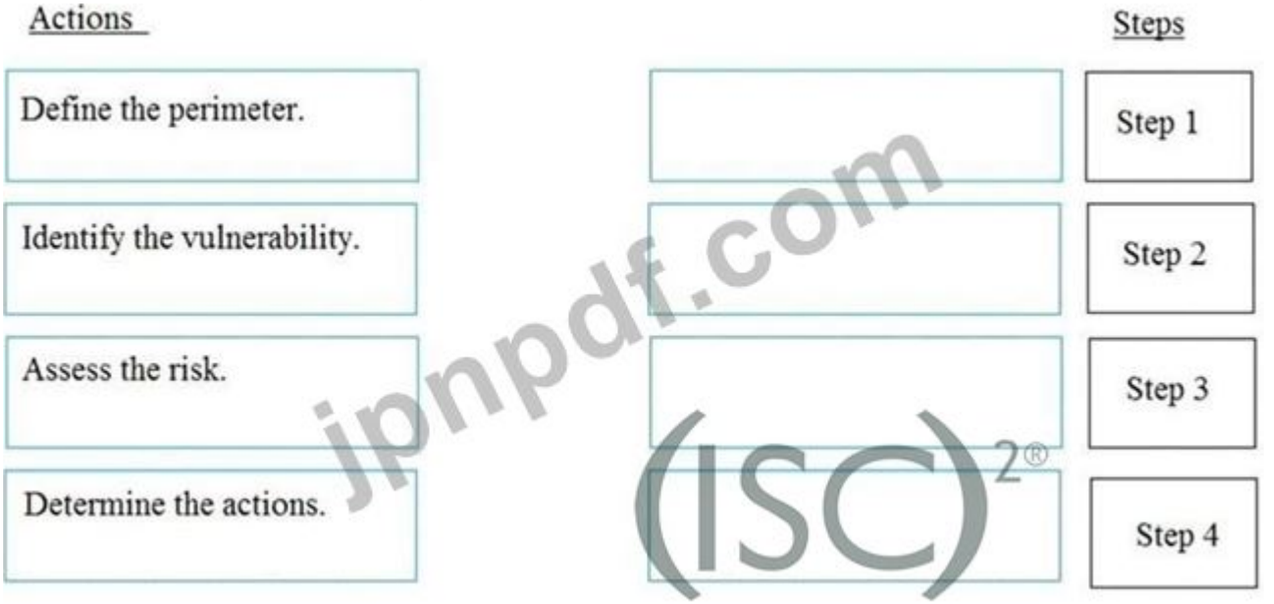
最新問題: **424**
次のうち、モーションディテクタのタイプではないものはどれですか？
A. 光電センサー
B. 波のパターン
C. 静電容量
D. オーディオ検出器
Answer: D (メーッセージを残す**)**
オーディオ検出器は動きではなく音を検出しますAではありません：光電センサーは、それが行うように設計された動きセンサーです。

最新問題: **425**
次の項目のうち、主に整合性を確保するために使用されていないものはどれですか？
A. 巡回冗長検査（CRC）
B. 安価なディスクの冗長アレイ（RAID）システム
C. ハッシュアルゴリズム
D. BibaSecurityモデル
Answer: B (メーッセージを残す**)**
説明/参照：
Explanation:
RAIDはフォールトトレランスに使用できますが、整合性は提供されません。
不正解：
A：巡回冗長検査(CRC)は整合性ツールとして機能します。
C：ハッシュ合計は整合性ツールとして機能します。
D：Bibaの整合性セキュリティモデルは整合性に重点を置いています。

参照：
Stewart、James M.、Ed Tittel、およびMike Chapple、CISSP：Certified Information Systems Security Professional Study Guide、第5版、Sybex、インディアナポリス、2011年、p。171

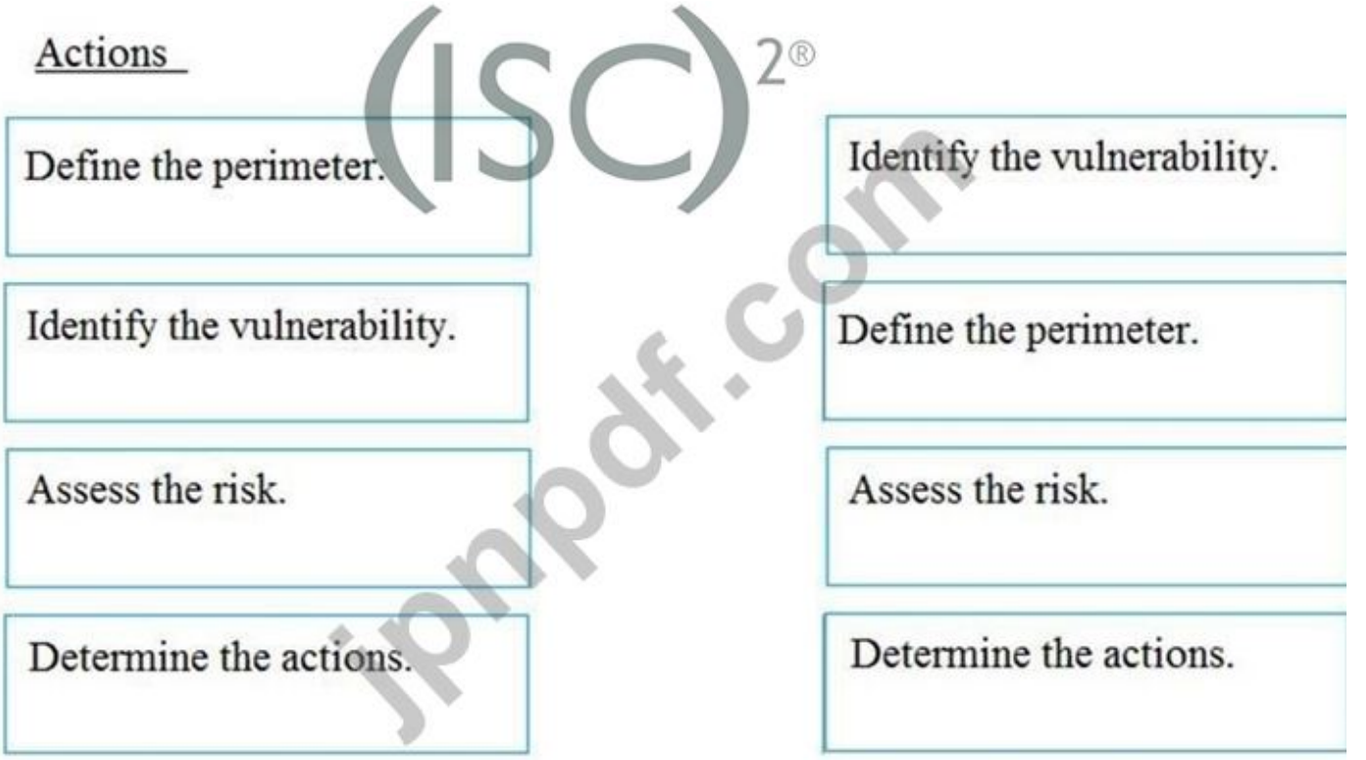
最新問題: **426**
緊急時対応計画の実施における最初のステップは、以下を実行することです。
A. ファームウェアのバックアップ
B. データのバックアップ
C. オペレーティングシステムソフトウェアのバックアップ
D. アプリケーションソフトウェアのバックアップ
Answer: (解答を表示する**)**
データのバックアップは、緊急時対応計画の最初のステップです。
データがなければ、処理するものは何もありません。「バックアップなし、リカバリなし」。
次に、ハードウェアのバックアップを行う必要があります。
必要に応じて、代替処理機能を正式に手配する必要があります。
発生します。
オペレーティングシステムとアプリケーションソフトウェアは、後で処理する必要があります。
出典：VALLABHANENI、S。Rao、CISSP Examination Textbooks、Volume 2：Practice、SRV Professional Publications、2002年、第8章、事業継続計画と災害復旧
計画（506ページ）。

最新問題: **427**
情報セキュリティ評価の正しい手順は何ですか？
情報セキュリティ評価手順を、左側の右側の番号付きボックスの横に正しい順序で配置します。



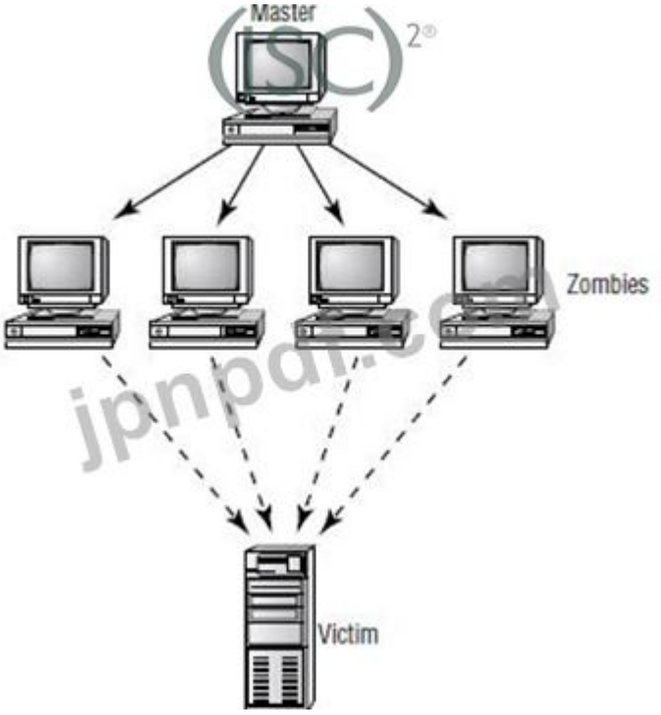
jpnpdf.com
(ISC)2®

Answer:
説明



最新問題: **428**

下の画像を表示して、攻撃を特定します



A. DDoS

B. DOS

C. TFN

D. リフレクション攻撃

Answer: (解答を表示する)

ネットワークに対して実行する最も簡単な攻撃は、過剰なトラフィックまたは 細工された」トラフィックによってネットワークを過負荷にして、ネットワークを混乱させてシャットダウンしたり、役に立たなくなったりすることです。
この画像は、分散型サービス拒否攻撃を示しています。この攻撃では、多くのコンピューターがあらゆる種類のトラフィックで被害者を攻撃し、ネットワーク上で通信したりサービスを提供したりできなくなります。
ネットワーク上のコンピューターは、他のコンピューターにサービスを提供できます。サーバーは特定のTCPまたはUDPポートをリッスンし、ソフトウェアはサーバー上のポートを開いて訪問者からのトラフィックを受け入れます。
そのサーバー上のサービスのほとんどのユーザーは正常に動作しますが、攻撃者がプロトコルスタック自体を介してサーバーのサービスまたはオペレーティングシステムを攻撃することにより、サーバーを攻撃して停止しようとする場合があります。
この質問の場合、被害者はゾンビからのサービス要求に縛られています。通常はUDPですが、多くの場合TCPトラフィックである可能性があり、残念ながらそのような攻撃を打ち負かすことはほぼ不可能です。
この攻撃を、自分の電話を使用できないという電話で誰かに何度も電話をかけることと比較することができますが、電話に特に破壊的なことは何もしていません。リソースを使い果たして、所有者が役に立たなくなっているだけです。
次の答えは正しくありません。
--DOS-サービス拒否 :これはほぼ正しいですが、単純なDOS攻撃は、あるコンピューターが別のコンピューターにフラッディングすることであり、DDoSで見られる多対1の攻撃ではないため間違っています。
--TFN --Tribe Flood Network攻撃 :これは、画像に具体的に描かれているものではないため、正解ではありません。TFNは、実際にはDDoS攻撃を実行するために使用されるソフトウェアです。攻撃そのものではありません。詳細はこちら。
-リフレクション攻撃 :リフレクション攻撃は、両方向で同じプロトコルを使用し、通常はゾンビを含まない認証システムに対する攻撃であるため、これは正解ではありません。
この質問を作成するために、次の参照が使用されました。
2013.公式セキュリティ+カリキュラム。
と
Hernandez CISSP、Steven（2012-12-21）。CISSP CBKの公式（ISC）2ガイド、サードEdition（ISC）2 Press）Kindle Locations 8494-8495）。AuerbachPublications。Kindle版。

最新問題: **429**
以下のどの選択がリスクの目標を最も正確に反映していますか
緩和？
A. 事業の混乱の影響を分析し、
会社の対応

B. セキュリティに対するすべての脆弱性と脅威を分析して削除する
組織内
C. 組織が許容できるリスクの許容レベルを定義し、そのレベルまでリスクを軽減する
D. 組織が許容できるリスクの許容レベルを定義し、損失または混乱に関連するコストを保険会社などのサードパーティに割り当てます。
Answer: C (メーッセージを残す**)**
正解は、 組織が許容できるリスクの許容レベルを定義し、そのレベルまでリスクを軽減する」です。リスク軽減の目標は、組織が許容できるレベルまでリスクを軽減することです。したがって、リスク分析、ビジネス影響評価、および/または脆弱性評価を通じて、組織のリスクを定義する必要があります。
組織内のセキュリティに対するすべての脆弱性と脅威を分析して削除する」という回答は不可能です。回答 組織が許容できるリスクの許容レベルを定義し、損失または混乱に関連するコストを保険会社などのサードパーティに割り当てること」は、リスク移転と呼ばれます。
回答 事業の混乱の影響を分析し、会社の対応を準備すること」は気を散らすものです。

最新問題**: 430**
データの機密性を保護するための最初のステップは次のうちどれですか？
A. ファイアウォールをインストールします
B. 暗号化を実装する
C. 機密情報を特定する
D. すべてのユーザーアクセス権を確認する
Answer: C (メーッセージを残す**)**
データの機密性を保護するため。
次の理由は正しくありません。
ファイアウォールのインストールは、情報が感度レベルで識別された後に行われるため、正しくありません。
暗号化の実装も正しくありません。これは、データが識別された後にデータを保護するメカニズムの1つであるためです。
これは識別された情報の保護メカニズムでもあるため、すべてのユーザーアクセス権の確認も正しくありません。
参照 :ションハリスAIO v3、第4章 :アクセス制御、ページ :126

最新問題**: 431**
組織のシステムが24時間以上使用できなくなるとすると、ディザスタリカバリ（DR）サイトの最も費用効果の高いソリューションは何でしょうか。
A. ウォームサイト
B. ホットサイト
C. ミラーサイト
D. コールドサイト

Answer: (解答を表示する**)**
セクション :セキュリティ運用

最新問題**: 432**
シングルサインオンの主な懸念事項は何ですか？
A. パスワードが開示された場合、最大の不正アクセスが可能になります。
B. セキュリティ管理者の作業負荷が増加します。
C. ユーザーのパスワードを覚えるのは難しいでしょう。
D. ユーザーのアクセス権が増加します。
Answer: A (メーッセージを残す**)**
説明/参照：
Explanation:
シングルサインオン $SO)の主な懸念事項は、ユーザーのIDとパスワードが侵害された場合、侵入者がユーザーに許可されたすべてのシステムにアクセスできるようになることです。
不正解：
B :セキュリティ管理者は複数のユーザーアカウントを1つだけ維持する責任を負わないため、セキュリティ管理者の作業負荷は減少し、増加しません。
C :ユーザーが覚えておくべきパスワードは1つだけなので、難しいことではありません。
D :ユーザーのアクセス権は、システムに手動でログインする必要がある場合と何ら変わりはありません。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、2013、pp.207-209

最新問題**: 433**
次のうち、最も単純なタイプのファイアウォールはどれですか？
A. ステートフルパケットフィルタリングファイアウォール
B. パケットフィルタリングファイアウォール
C. デュアルホームホストファイアウォール
D. アプリケーションゲートウェイ
Answer: B (メーッセージを残す**)**
静的パケットフィルタリングファイアウォールは、最も単純で最も安価なタイプのファイアウォールであり、リスクの低いコンピューティング環境に最小限のセキュリティ対策を提供します。静的パケットフィルタファイアウォールは、着信データパケットの送信元アドレスと宛先アドレスの両方を調べて、ACLをそれらに適用します。これらは、ネットワーク層またはトランスポート層のいずれかで動作します。それらは、第1世代のファイアウォールとして知られています。パケットフィルターのみであった古いファイアウォールは、基本的に、ホストアドレスと通信セッションにアクセス制御機能を提供するルーティングデバイスでした。これらのデバイスは、ステートレスインスペクションファイアウォールとも呼ばれ、ファイアウォールを通過するトラフィックの各フローの状態を追跡しません。これは、たとえば、単一のセッション内の複数の要求を相互に関連付けることができないことを意味します。パケットフィルタリングは、ほとんどの

最新のファイアウォールの中核ですが、ステートレスパケットフィルタリングのみを実行するファイアウォールは、現在販売されているものはほとんどありません。より高度なフィルターとは異なり、パケットフィルターはパケットの内容を考慮しません。それらのアクセス制御機能は、ルールセットと呼ばれる一連のディレクティブによって制御されます。パケットフィルタリング機能は、ルーティングが可能なほとんどのオペレーティングシステムとデバイスに組み込まれています。純粋なパケットフィルタリングデバイスの最も一般的な例は、アクセス制御リストを使用するネットワークルーターです。パケットフィルタリング機能は、ルーティングが可能なほとんどのオペレーティングシステムとデバイスに組み込まれています。純粋なパケットフィルタリングデバイスの最も一般的な例は、アクセス制御リストを使用するネットワークルーターです。パケットフィルタリング機能は、ルーティングが可能なほとんどのオペレーティングシステムとデバイスに組み込まれています。純粋なパケットフィルタリングデバイスの最も一般的な例は、アクセス制御リストを使用するネットワークルーターです。

ファイアウォールには多くの種類があります。アプリケーションレベルのファイアウォール-プロキシサーバーと呼ばれることもあります。これは、受け入れられた各データパケットのコピーを1つのネットワークから別のネットワークに転送することによって機能します。それらは第2世代のファイアウォールとして知られています。アプリケーションプロキシゲートウェイは、下位層のアクセス制御と上位層の機能を組み合わせた高度なファイアウォールの機能です。これらのファイアウォールには、相互に通信したい2つのホスト間の仲介役として機能するプロキシエージェントが含まれており、それらの間の直接接続は許可されません。接続が成功するたびに、実際には2つの別々の接続が作成されます。1つはクライアントとプロキシサーバーの間、もう1つはプロキシサーバーと実際の宛先の間です。プロキシは、2つのホストに対して透過的であることが意図されています。それらの観点からは、直接接続があります。外部ホストはプロキシエージェントとのみ通信するため、内部IPアドレスは外部からは見えません。プロキシエージェントはファイアウォールルールセットと直接インターフェイスして、ネットワークトラフィックの特定のインスタンスがファイアウォールを通過できるようにするかどうかを決定します。ステートフルインスペクションファイアウォール-パケットは、ネットワークレイヤーで動作するインスペクションエンジンによってキャプチャされ、すべてのレイヤーで分析されます。それらは第3世代のファイアウォールとして知られています。ステートフルインスペクションは、接続の状態を追跡し、期待される状態から逸脱するパケットをブロックすることにより、パケットフィルターの機能を改善します。これは、トランスポート層の認識を高めることによって実現されます。パケットフィルタリングと同様に、ステートフルインスペクションは、ネットワーク層でパケットをインターセプトし、既存のファイアウォールルールで許可されているかどうかを確認しますが、パケットフィルタリングとは異なり、ステートフルインスペクションは状態テーブル内の各接続を追跡します。状態テーブルエントリの詳細はファイアウォール製品によって異なりますが、通常、送信元IPアドレス、宛先IPアドレス、ポート番号、および接続状態情報が含まれます。

Webアプリケーションファイアウォール-Webサーバーで使用されるHTTPプロトコルは
悪意のあるソフトウェアを誰かのコンピュータに配置するなど、さまざまな方法で攻撃者
Webを閲覧したり、人をだまして、持っていない可能性のある個人情報を公開させたりする

それ以外は。これらのエクスプロイトの多くは、Webと呼ばれる特殊なアプリケーションファイアウォールによって検出できます。
Webサーバーの前にあるアプリケーションファイアウォール。
Webアプリケーションファイアウォールは、他のファイアウォールと比較して、比較的新しいテクノロジーです。
テクノロジー、およびそれらが軽減する脅威の種類は、依然として頻繁に変化しています。なぜなら彼ら
サーバーへの攻撃を防ぐためにWebサーバーの前に配置され、多くの場合、
従来のファイアウォールとは大きく異なります。
ホストベースのファイアウォールとパーソナルファイアウォールサーバーとパーソナル用のホストベースのファイアウォール
デスクトップおよびラップトップのパーソナルコンピューター（PC）用のファイアウォールは、セキュリティの追加レイヤーを提供します
ネットワークベースの攻撃に対して。これらのファイアウォールはソフトウェアベースであり、それらが存在するホスト上に存在します
保護それぞれが単一のホストの着信および発信ネットワークトラフィックを監視および制御します。
特定のニーズを満たすために、ネットワークファイアウォールよりもきめ細かい保護を提供できます
ホスト。
ホストベースのファイアウォールは、Linux、Windows、
Solaris、BSD、およびMac OS X Serverであり、サードパーティのアドオンとしてインストールすることもできます。
サーバーへの必要なトラフィックのみを許可するようにホストベースのファイアウォールを構成すると、保護が提供されます
同じサブネットまたは他の内部のホストを含む、すべてのホストからの悪意のあるアクティビティに対して
ネットワークファイアウォールによって分離されていないサブネット。サーバーからの送信トラフィックを制限することもできます
ホストに感染する特定のマルウェアが他のホストに広がるのを防ぐのに役立ちます。11ホスト-ベースのファイアウォールは通常、ロギングを実行し、多くの場合、アドレスベースを実行するように構成できます。
およびアプリケーションベースのアクセス制御
動的パケットフィルタリング適用するACLについて情報に基づいた決定を行います。彼らはとして知られています
第4世代のファイアウォール。
カーネルプロキシモジュラーカーネルベースのマルチレイヤーを提供する非常に特殊なアーキテクチャ
評価し、NTエグゼクティブスペースで実行されます。彼らは第5世代として知られています
ファイアウォール。

以下は間違った答えでした：
リストされている他のすべてのタイプのファイアウォールは、パケットフィルタリングファイアウォールよりも複雑です。
この質問に使用される参照：
HARRIS、ション、オールインワンCISSP認定試験ガイド、第6版、電気通信およびネットワークセキュリティ、630ページ。
と
ファイアウォールおよびファイアウォールポリシーに関するNISTガイドライン、特別刊行物800-4改訂1

最新問題: **434**
法的領域内で、証拠がどのように収集されたかの合法性に関係する規則は何ですか？
A. 除外規則
B. 最良証拠の原則
C. 伝聞規則
D. 調査ルール
Answer: A (メーッセージを残す**)**
説明/参照：
Explanation:
除外規則は、証拠を合法的に収集する必要があること、または証拠を使用できないことを示しています。法執行官が不当な捜索や押収から解放されるという容疑者の権利を侵害して証拠を不法に押収したという連邦憲法に基づく原則は、刑事訴追において容疑者に対して使用することはできません。除外規則は、刑事被告の修正第4条の権利に違反して得られた証拠を除外するように設計されています。憲法修正第4条は、法執行官による不当な捜索や押収から保護します。犯罪容疑者の捜索が不合理である場合、捜索で得られた証拠は裁判から除外されます。除外規則は法廷で作成された規則です。これは、立法機関によって可決された法令ではなく、米国によって作成されたことを意味します 最高裁判所。除外規則は、憲法修正第4条により連邦裁判所に適用されます。裁判所は、第14修正条項の適正手続き条項にもかかわらず、州裁判所に適用されるとの判決を下しました。（権利章典最初の10の修正は連邦政府による行動に適用されます。裁判所が保持している第14の修正は、権利章典の保護のほとんどを州による行動に適用できるようにします。）
除外規則は1900年代初頭から存在しています。規則が作成される前は、裁判官が証拠が適切であると判断した場合、刑事裁判で証拠は許容されていました。証拠が押収された方法は問題ではありませんでした。これは1914年に米国が変化し始めました
最高裁判所は、憲法修正第4条を施行する方法を考案しました。ウィークス対合衆国、232 US 383、34S.Ct。341、58L.Ed。652（1914）、連邦捜査官はフリーモントウィークの家でギャンブルの証拠を不当に捜索しました。捜査で押収された証拠は裁判で使用され、ウィークスは有罪判決を受けた。上訴において、裁判所は、憲法修正第4条が無保証の捜査を通じて確保された証拠の使用を禁じていると判示した。数週間の信念が逆転したため、排除規則が生まれました。最良証拠の原則は、変更の可能性を制限することに関するものです。最良証拠の原則は、少なくとも18世紀までさかのぼることができるコモンローの証拠規則です。Omychund v Barker（1745）1 Atk、21、49; 26

ER 15、33、ハーウィック卿は、 事件の性質が許す限り最高」でない限り、証拠は許容されないと述べた。一般的なルールは、その二次証拠、コピーやファクシミリなど、元の文書が存在する場合は許容されず、破壊または利用できないことを示すその他の状況のために利用できません。最良証拠の原則の理論的根拠は、それが生じた文脈から理解することができます。18世紀には、通常、書記官 または訴訟当事者）が手作業でコピーを作成していました。最良証拠の原則は、原本が作成されなかった場合、そのようなコピーに依存することでエラーまたは詐欺の重大な可能性があるという仮定に基づいていました。伝聞規則は、コンピューターで生成された証拠に関するものであり、これは中古の証拠と見なされます。伝聞は、ある出来事、状態、または最初の人が直接経験したことのないものに関して、ある人から別の人によって収集された情報です。証拠として提出された場合、そのような陳述は伝聞証拠と呼ばれます。法的な用語として、 伝聞」は、主張されていることの真実を証明する証拠などの情報の使用のより狭い意味を持つこともできます。法廷でのそのような 伝聞証拠」の使用は、一般的に許可されていません。この禁止は伝聞規則と呼ばれます。たとえば、目撃者は 「スーザンはトムが町にいると私に言った」と言います。目撃者はトムが町にいるのを見なかったので、声明はトムが町にいたという事実の伝聞証拠であり、許容されません。しかし、スーザンがトムが町にいると言ったことの証拠として、そして彼が町にいるかどうかについての彼女の知識の問題については許容されるでしょう。伝聞証拠には多くの例外規則があります。法廷での使用は一般的に許可されていません。この禁止は伝聞規則と呼ばれます。たとえば、目撃者は 「スーザンはトムが町にいると私に言った」と言います。目撃者はトムが町にいるのを見なかったので、声明はトムが町にいたという事実の伝聞証拠であり、許容されません。しかし、スーザンがトムが町にいると言ったことの証拠として、そして彼が町にいるかどうかについての彼女の知識の問題については許容されるでしょう。伝聞証拠には多くの例外規則があります。法廷での使用は一般的に許可されていません。この禁止は伝聞規則と呼ばれます。たとえば、目撃者は 「スーザンはトムが町にいると私に言った」と言います。目撃者はトムが町にいるのを見なかったので、声明はトムが町にいたという事実の伝聞証拠であり、許容されません。しかし、スーザンがトムが町にいると言ったことの証拠として、そして彼が町にいるかどうかについての彼女の知識の問題については許容されるでしょう。伝聞証拠には多くの例外規則があります。そして彼が町にいたかどうかについての彼女の知識の問題について。伝聞証拠には多くの例外規則があります。そして彼が町にいたかどうかについての彼女の知識の問題について。伝聞証拠には多くの例外規則があります。

試験の目的のために、あなたは伝聞証拠に対する業務記録の例外規則に精通している必要があります。通常の業務過程で作成された業務記録は信頼できると見なされ、記録が証拠に導入されたときに適切な基盤が確立されていれば、通常、この例外の下で持ち込むことができます。事件がどの管轄区域にあるかに応じて、記録管理者または記録の知識を持った誰かが記録の基礎を築く必要があります。定期的に実行されるドキュメントビジネスプロセスの一部として収集されるログは、この例外に該当します。それらは法廷で提示される可能性があり、伝聞とは見なされません。

参照 :ROTHKE、Ben、CISSPCBKドメイン9のレビュープレゼンテーション。

http://legal-dictionary.thefreedictionary.com/Exclusionary+Rule

http://en.wikipedia.org/wiki/Exclusionary_rule

http://en.wikipedia.org/wiki/Hearsay_in_United_States_law#Hearsay_exceptions

最新問題: **435**
企業は、企業に導入された資産の保守を開始する必要があると判断しました。
会社をコンプライアンスに準拠させるために所有権情報を決定および維持するには、どのようなアプローチに従う必要がありますか？
A. エンタープライズ資産管理フレームワーク
B. 市販のソフトウェアを使用した資産ベースライン
C. アセットへのアクティブなユーザーログインを報告するスクリプト
D. ドメインログインレコードを使用した資産所有権データベース
Answer: (解答を表示する**)**

最新問題: **436**
次の暗号化アルゴリズムのうち、離散対数を処理しないものはどれですか？
A. エルガマル
B. Diffie-Hellman
C. RSA
D. 楕円曲線
Answer: (解答を表示する**)**
説明/参照：
Explanation:
RSAは離散対数を扱いません。
RSAは、発明者のRon Rivest、Adi Shamir、Leonard Adlemanにちなんで名付けられたもので、非対称アルゴリズムに関して最も人気のある公開鍵アルゴリズムです。RSAは世界的な事実上の標準であり、デジタル署名、鍵交換、および暗号化に使用できます。1978年にMITで開発され、認証とキー暗号化を提供します。
このアルゴリズムの安全性は、元の素数に大きな数を因数分解することの難しさに由来します。公開鍵と秘密鍵は大きな素数のペアの機能であり、秘密鍵を使用して暗号文から平文にメッセージを復号化するために必要なアクティビティは、製品を2つの素数に分解することに相当します。
不正解：
A：El Gamalは、デジタル署名、暗号化、および鍵交換に使用できる公開鍵アルゴリズムです。これは、大きな数を因数分解することの難しさではなく、有限体で離散対数を計算することに基づいています。
B：Diffie-Hellmanアルゴリズムを使用すると、2つのシステムで、事前の関係や事前の取り決めを必要とせずに、対称鍵を安全に生成できます。このアルゴリズムではキーの配布が可能ですが、暗号化またはデジタル署名機能は提供されません。このアルゴリズムは、有限体で離散対数を計算することの難しさに基づいています。
D：楕円曲線アルゴリズムは、楕円曲線の離散対数を計算します。これは、有限体での離散対数の計算とは異なります。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、2013、pp.815、818

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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: **437**
水はどの火災クラスに最も適していますか？
A. クラスAの火災
B. クラスBの火災
C. クラスDの火災
D. クラスCの火災
Answer: (解答を表示する**)**

最新問題: **438**
ディザスタリカバリプラン（DRP）のテストについて正しいのは次のうちどれですか？
A. 災害計画全体をテストできるようになるまで、テストを実行しないでください。
B. テストのコンポーネントが失敗した場合でも、テストを続行する必要があります。
C. すべてのテストに合格すれば、会社は災害に完全に備えることができます。
D. 通常、運用ネットワークはテスト中にシャットダウンされます。
Answer: (解答を表示する**)**

最新問題: **439**
現代のコンピューターのマザーボードにインストールされ、対称および非対称のキー、ハッシュ、デジタル証明書の保存と処理を含むセキュリティ機能の実行に専念しているマイクロチップとは何ですか。
A. トラステッドプラットフォームモジュール（TPM）
B. トラステッドBIOSモジュール（TBM）
C. 中央処理装置（CPU）
D. 算術論理演算装置（ALU）
Answer: A (メーッセージを残す**)**
トラステッドプラットフォームモジュール（TPM）は、トラステッドコンピューティングによって考案されました
Group（TCG）は、セキュリティの弱点や攻撃に対してコンピューティングプラットフォームを強化するために、オープンスタンダードを推進する組織です。
TPMは基本的に、暗号化機能を実行するためのモジュールが追加された、安全に設計されたマイクロコントローラーです。

これらのモジュールにより、暗号化キー、ハッシュ値、および疑似番号シーケンスの高速化およびストレージ処理が可能になります。
TPMの内部ストレージは、不揮発性ランダムアクセスメモリに基づいています。このメモリは、電源がオフになっても情報を保持するため、不揮発性と呼ばれます。TPMは、システム構成を改ざんしようとする試みを阻止するために使用されます。
次の答えはすべて正しくありません。
Trusted BIOS Module（TBM）これは偽の気を散らすものです。
中央処理装置（CPU）中央処理装置CPU）（以前は中央処理装置とも呼ばれていました）は、基本的な算術、論理、および入力を実行することによってコンピューター・プログラムの命令を実行するコンピューター内のハードウェアです。システムの出力操作。この用語は、少なくとも1960年代初頭から、コンピュータ業界で使用されています。CPUの形式、設計、および実装は、その歴史の中で変化しましたが、基本的な動作はほとんど変わりません。
算術論理演算装置（ALU）デジタル電子機器では、算術論理演算装置（ALU）は、整数の算術演算と論理演算を実行するデジタル回路です。ALUは、コンピューターの中央処理装置の基本的な構成要素であり、最も単純なマイクロプロセッサーでさえ、タイマーの保守などの目的でALUを備えています。最新のCPUおよびグラフィックスプロセッシングユニット（GPU）内にあるプロセッサは、非常に強力で非常に複雑なALUに対応しています。1つのコンポーネントに複数のALUが含まれる場合があります。
この質問を作成するために、次の参照が使用されました。
ハリス、ション（2012-10-18）。CISSPオールインワン試験ガイド、第6版（p.843）。マグロウ-丘。キンドル版。
http://en.wikipedia.org/wiki/Central_processing_unit
http://en.wikipedia.org/wiki/Arithmetic_logic_unit

最新問題: **440**
3つ以上の実行ドメインまたは特権レベルがあるアーキテクチャは次のように呼ばれます。
A. リングレイヤー
B. ネットワーク環境。
C. セキュリティモデル
Answer: A (メーッセージを残す**)**
コンピュータサイエンスでは、保護リングと呼ばれることが多い階層型保護ドメインは、データと機能をフォールト（フォールトトレランス）および悪意のある動作（コンピュータセキュリティ）から保護するメカニズムです。このアプローチは、機能ベースのセキュリティのアプローチとは正反対です。
コンピュータオペレーティングシステムは、リソースへのさまざまなレベルのアクセスを提供します。保護リングは、コンピュータシステムのアーキテクチャ内の2つ以上の階層レベルまたは特権の層の1つです。これは通常、ハードウェアまたはマイクロコードレベルでさまざまなCPUモードを提供する一部のCPUアーキテクチャによってハードウェアで強制されます。リングは、最小

特権（最も信頼され、通常はゼロの番号が付けられます）から最小特権までの階層に配置されます。
（信頼性が最も低く、通常はリング番号が最も高くなります）。ほとんどのオペレーティングシステムでは、リング0は最も多くの特権を持つレベルであり、CPUやメモリなどの物理ハードウェアと最も直接対話します。
リング間に特別なゲートが用意されており、任意の使用を許可するのではなく、事前定義された方法で外部リングが内部リングのリソースにアクセスできるようになっています。リング間のアクセスを正しくゲーティングすると、あるリングまたは特権レベルのプログラムが別のリングのプログラム用のリソースを悪用するのを防ぐことで、セキュリティを向上させることができます。たとえば、リング3でユーザープログラムとして実行されているスパイウェアは、ハードウェアアクセスがデバイスドライバー用に予約されたリング1機能である必要があるため、ユーザーに通知せずにWebカメラをオンにしないようにする必要があります。番号の大きいリングで実行されているWebブラウザなどのプログラムは、ネットワークへのアクセスを要求する必要があります。これは、番号の小さいリングに制限されているリソースです。
リングアーキテクチャ
他のすべての答えは、中傷者であるため正しくありません。
参照：
OIG CBKのセキュリティアーキテクチャとモデル（311ページ）
と
https://en.wikipedia.org/wiki/Ring_%28computer_security%29

最新問題: **441**
次のルールのうち、最小特権の概念をサポートする可能性が最も低いのはどれですか？
A. 管理アカウントの数は最小限に抑える必要があります。
B. 管理者は、メールの読み取りなどの日常的な操作を実行するときに、通常のアカウントを使用する必要があります。
C. ハッカーが使用する可能性のあるツールのアクセス許可は、可能な限り制限する必要があります。
D. 重要なシステムおよびアプリケーションとの間のデータのみがファイアウォールの通過を許可される必要があります。
Answer: D (メーッセージを残す**)**
説明/参照：
Explanation:
重要なシステムやアプリケーションとの間のデータのみがファイアウォールの通過を許可されるべきです。重要なシステムまたはアプリケーションは、必ずしもトラフィックがファイアウォールを通過する必要はありません。
たとえそうだったとしても、最低限必要なサービスだけが許可されるべきです。重要と見なされないシステムでも、トラフィックがファイアウォールを通過する必要がある場合があります。
最小特権は、コンピューターセキュリティの基本原則です。つまり、ユーザーには、自分の仕事やタスクを実行するために必要な権限のみを付与する必要があります。最小特権とは、タスクを実

行するために必要な最小限の特権を確実に持つことです。管理者アカウントを使用して電子メールをチェックしていない管理者は、この明確な例です。
不正解：
A：管理アカウントの数は最小限に抑える必要があります。これは適切な方法であり、最小特権の概念をサポートします。
B：管理者は、メールの読み取りなどの日常的な操作を実行するときに通常のアカウントを使用する必要があります。これは適切な方法であり、最小特権の概念をサポートします。
C：ハッカーが使用する可能性のあるツールのアクセス許可は、可能な限り制限する必要があります。これは適切な方法であり、最小特権の概念をサポートしています。

最新問題: **442**
脅威とリスクの分析に関する意思決定支援システム（DSS）の特徴は次のうちどれですか？
A. DSSは、高度に構造化された問題を解決することを目的としています。
B. DSSは、ユーザーの意思決定アプローチにおける柔軟性を強調しています。
C. DSSは、構造化された意思決定タスクのみをサポートします。
D. DSSは、モデルの使用と従来とは異なるデータアクセスおよび取得機能を組み合わせたものです。
Answer: B (メーッセージを残す**)**
DSSは、ユーザーの意思決定アプローチにおける柔軟性を強調しています。これは、構造化されていない問題を解決することを目的としており、モデルと分析手法の使用を従来のデータアクセスおよび取得機能と組み合わせ、半構造化された意思決定タスクをサポートします。
DSSは、デルファイ法またはデルファイ法と呼ばれることもあります。
デルファイ法は、各メンバーが特定の脅威の結果がどうなると思うかについて正直な意見を確実に与えるために使用されるグループ決定方法です。これにより、個人のグループが他の人の思考プロセスに沿って進むようにプレッシャーを感じることを回避し、独立した匿名の方法で参加できるようになります。グループの各メンバーは、特定の脅威について自分の意見を提供し、分析を実行しているチームにそれを提出します。結果はまとめられてグループメンバーに配布され、グループメンバーはコメントを匿名で書き留めて分析グループに返します。
コンセンサスが形成されるまで、コメントは編集され、さらにコメントのために再配布されます。この方法は、個人が口頭で同意する必要なしに、コスト、損失値、および発生確率に関する合意を取得するために使用されます。
これが主題のISC2本の報道です：
情報の評価に関連してコンセンサスを使用する方法の1つは、コンセンサス/修正されたデルファイ法です。評価演習の参加者は、議論されているタスクについて匿名でコメントするよう求められます。この情報は収集され、元の作成者以外の参加者に配布されます。この参加者は、原作者の観察についてコメントします。収集された情報は公開フォーラムで議論され、最良のコースはグループによって合意されます（コンセンサス）。
試験のヒント：
DSSは、一部の書籍でDelphiメソッドまたはDelphiと呼ばれているものです。

技術。試験の目的のために両方の用語に精通してください。
他の答えは正しくありません：
DSSは高度に構造化された問題を解決することを目的としています」は、構造化されていない問題を解決することを目的としているため、正しくありません。
DSSは構造化された意思決定タスクのみをサポートする」も、半構造化された意思決定タスクをサポートするため、正しくありません。
DSSは、モデルの使用と非従来型のデータアクセスおよび取得機能を組み合わせたもの」も、モデルおよび分析手法の使用と従来のデータアクセスおよび取得機能を組み合わせたものであるため、正しくありません。
この質問に使用される参照：
ハリス、ション（2012-10-25）。CISSPオールインワン試験ガイド、第6版（p.91）。マグロウヒル。キンドル版。
と
シュナイター、アンドリュー（2013-04-15）。CISSP CBK、第3版の公式（ISC）2ガイド：情報セキュリティガバナンスとリスク管理（ISC）2 Press）Kindleの場所1424-1426）。AuerbachPublications。キンドル版。

最新問題: **443**
次のうち、一般的なバックアップ方法ではないものはどれですか？
A. 完全バックアップ方式
B. 毎日のバックアップ方法
C. 増分バックアップ方式
D. 差分バックアップ方式
Answer: B (メーッセージを残す**)**
毎日のバックアップはバックアップ方法ではありませんが、バックアップが作成される周期性を定義します。毎日の完全バックアップ、増分バックアップ、または差分バックアップがあります。
出典：KRUTZ、Ronald L.＆VINES、Russel D.、CISSP Prep Guide：Mastering the Ten Domains of Computer Security、John Wiley＆Sons、2001、Chapter 3：Telecommunications and Network Security（69ページ）。

最新問題: **444**
UTPカテゴリの評価では、風が強くなります。
A. 定格が高く、干渉やクロストークに対する耐性が高い。
B. 定格が遅くなり、干渉や減衰に対する耐性が低下します。
C. 定格が短く、干渉や減衰に対する耐性があります。
D. 定格が長くなり、干渉や減衰に対する耐性が高くなります。
Answer: A (メーッセージを残す**)**
説明/参照：
Explanation:

UTPカテゴリを増やすと、信号の伝送が向上します。つまり、ケーブルは干渉やクロストークに対する耐性が高くなります。
最も低いカテゴリは1で、最も高いカテゴリは8.2です。
不正解：
B :UTPカテゴリは、1から8.2までの数字です。それらは速度を表すものではありません。
C :UTPカテゴリは単なる数字です。それらは長さを表すものではありません。
D :UTPカテゴリは単なる数字です。それらは速度を表すものではありません。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、New York、2013、p。559

最新問題**: 445**
次のうち、VPN通信プロトコル標準ではないものはどれですか？
A. ポイントツーポイントトンネリングプロトコル（PPTP）
B. チャレンジハンドシェイク認証プロトコル（CHAP）
C. レイヤー2トンネリングプロトコル（L2TP）
D. IPセキュリティ
Answer: B (メーッセージを残す**)**
CHAPは、ユーザーのパスワードを暗号化するポイントツーポイントプロトコル接続の認証メカニズムです。これは、3ウェイハンドシェイクを使用するプロトコルです。サーバーはクライアントにチャレンジを送信します。これには、リプレイ攻撃を阻止するためのランダムな値（ナンス）が含まれます。クライアントは、ナンスとパスワードのMD5ハッシュで応答します。クライアントの応答がサーバーが期待したものである場合、認証は成功します。
上記のVPN通信プロトコル標準はPPTP、L2TP、IPSecです。
PPTPとL2TPは、OSIモデルのデータリンク層（レイヤー2）で動作し、セッションごとに1つのポイントツーポイント接続のみを有効にします。
以下は不正解です。
PPTPは、ネイティブのPPP認証および暗号化サービスを使用します。ポイントツーポイントトンネリング
プロトコル（PPTP）は、他のプロトコル上で実行されるVPNプロトコルです。PPTPは、汎用ルーティングカプセル化（GRE）に依存して、エンドポイント間にトンネルを構築します。ユーザーが認証した後、通常はMicrosoft Challenge Handshake Authentication Protocolバージョン
2（MSCHAPv2）を使用して、Point-to-Point Protocol（PPP）セッションが以下を使用してトンネルを作成します。
GRE。
L2TPは、PPTPと以前のレイヤー2転送プロトコル（L2F）を組み合わせたものです。レイヤー2トンネリングプロトコル（L2TP）は、シスコのレイヤ2フォワーディング（L2F）とマイクロソフトのレイヤ2フォワーディング（L2F）のハイブリッドです。
PPTP。これにより、PPPを使用するシリアル回線を介した発信者は、インターネットを介してリモートネットワークに接続できます。ダイヤルアップユーザーは、PPP接続を使用してISPの

L2TPアクセスコンセントレーター（LAC）に接続します。LACは、PPPパケットをL2TPにカプセル化し、リモートネットワークのレイヤー2ネットワークサーバー（LNS）に転送します。この時点で、LNSはダイヤルアップユーザーを認証します。認証が成功すると、ダイヤルアップユーザーはリモートネットワークにアクセスできるようになります。
IPSecはネットワーク層（層3）で動作し、複数の同時トンネルを有効にします。IPセキュリティ（IPSec）は、認証と暗号化のメカニズムを提供することにより、IPと安全に通信するための一連のプロトコルです。IPSecの実装は必須です
IPv6、および多くの組織がIPv4を介してIPv6を使用しています。さらに、IPSecは2つのモードで実装できます。1つはエンドツーエンドの保護に適しており、もう1つはネットワーク間のトラフィックを保護します。
この質問に使用される参照：
Hernandez CISSP、Steven（2012-12-21）。CISSP CBKの公式（ISC）2ガイド、サードEdition（ISC）2 Press）Kindle Locations 7067-7071）。AuerbachPublications。Kindle版。
と
Hernandez CISSP、Steven（2012-12-21）。CISSP CBKの公式（ISC）2ガイド、サードEdition（ISC）2 Press）Kindle Locations 6987-6990）。AuerbachPublications。Kindle版。

最新問題: **446**
グローバルな組織は、リモートアクセス用の多要素認証ソリューションの一部としてハードウェアトークンを実装したいと考えています。この実装の主な利点は次のとおりです。
A. 不正アクセスから保護します。
B. エンドユーザーの説明責任の向上。
C. トークン登録のスケーラビリティ。
D. ユーザーアクセス管理を簡素化します。
Answer: A (メーッセージを残す**)**

最新問題: **447**
クラウドサービスは、ユーザーからオンおよびセキュリティへのセキュリティアサーションマークアップ言語（SAML）アサーションを受け入れます。ただし、攻撃者はネットワーク上の登録済みアカウントをスプーフィングし、SAMLプロバイダーにクエリを実行することができました。
この欠陥に対する最も一般的な攻撃のレバレッジは何ですか？
A. 攻撃者は、別のユーザーとして認証する要求を偽造します。
B. 攻撃者は、セキュリティドメイン間で認証および承認データを交換します。
C. 攻撃者は、同じユーザーとして繰り返し認証することにより、セキュリティドメインに対してサービス拒否（DoS）を実行します。
D. 攻撃者はSAMLアサーションを利用して、セキュリティドメインにアカウントを登録します。
Answer: (解答を表示する**)**

最新問題: **448**
バックアップ方式タイプではないものはどれですか？
A. インクリメンタル
B. リアクティブ
C. フル
D. ディファレンシャル
Answer: B (メーッセージを残す**)**
正解はリアクティブです。リアクティブはバックアップ方法ではありません。

最新問題: **449**
ソフトウェアライセンス違反を防ぐための最良の方法は次のうちどれですか？
A. 著作権侵害とソフトウェアの使用に関する企業ポリシーの実施。
B. すべてのPCがディスクレスワークステーションである必要があります。
C. LANにメータリングソフトウェアをインストールして、メータリングされたソフトウェアを介してアプリケーションにアクセスできるようにします。
D. 使用済みのPCを定期的にスキャンして、ソフトウェアの不正なコピーがPCにロードされていないことを確認します。
Answer: D (メーッセージを残す**)**
PC（特にインターネットからダウンロード）に適切なライセンスなしでソフトウェアをインストールするユーザーのすべての努力を制御することは不可能であるため、ライセンス違反を防ぐ最善の方法は、すべてのユーザーPCを定期的に監査して、インストールされているものを確認することです。プログラムとその性質（シェアウェア、フリーウェア、ライセンス）。すべてのアプリケーションがネットワーク対応であるとは限らないため、LAN監視ソフトウェアを使用することはできません。また、通常、ソフトウェアのインストールに関するポリシーがありますが、ユーザーはそれらに何度も依存することはありません。また、ソフトウェアライセンス違反を犯したユーザーを罰することも非常に良い習慣です。

最新問題: **450**
コンピューターで生成された証拠が考慮されます：
A. 最良の証拠
B. 中古の証拠
C. 実証的な証拠
D. 直接的な証拠
Answer: (解答を表示する**)**
説明/参照：
Explanation:
コンピューターで生成された証拠は、正確で信頼できることを証明できないため、通常、伝聞証拠または中古証拠のカテゴリーに分類されます。米国連邦証拠規則の下では、伝聞証拠は一般に法廷で許容されません。最良の証拠は、証拠のコピーまたは複製ではなく、元の証拠または一次証拠

です。コンピューターで生成された証拠には適用されません。直接の証拠は、証人による口頭の証言です。実証的な証拠は、陪審員を支援するために使用されます（モデル、イラスト、チャート）。
参考資料：KRUTZ、Ronald L.＆VINES、Russel D.、CISSP Prep Guide：Mastering the Ten Domains of Computer Security、John Wiley＆Sons、2001、Chapter 9：Law、Investigation、and Ethics（page310）。
ROTHKE、Ben、CISSPCBKドメイン9のレビュープレゼンテーション。

最新問題: **451**
メッセージと同じ長さのキーを使用するものは何ですか？
A. 実行中のキー暗号
B. ワンタイムパッド
C. ステガノグラフィ
D. 暗号ブロック連鎖
Answer: B (メーッセージを残す)
ワンタイムパッドは最も安全で、すべての暗号化方式の中で最も単純なものの1つです。第一次世界大戦直後にギルバートによって発明され、特許を取得しました
Vernam（AT＆Tの）とJoseph Mauborgne（USA、後にSignal Corpsのチーフ）。基本的な機能は、送信者と受信者がそれぞれ暗号化キーのコピーを持っていることです。これは、暗号化されるメッセージと同じ長さであり、各キーは1つのメッセージにのみ使用されてから破棄されます。そのキーはランダムである必要があり、パターンがなく、攻撃者には知られていない必要があります。さらに、キーを再利用してはなりません。再利用しないと、暗号が簡単に解読可能になります。その特徴の1つはキーの長さであり、メッセージと同じです。

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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: **452**
次のうち、リレーショナルデータベースのテーブルの行を表すものはどれですか？
A. レコードまたはタプル
B. 属性
C. 関係
D. 記録保持
Answer: A (メーッセージを残す)

最新問題: **453**

正しいテキスト
国際標準化機構/オープンシステム相互接続（ISO / OSI）レイヤー6は、次のうちどれですか？（空欄を埋める）
Answer:

最新問題: **454**
非随意アクセス制御。中央機関は、組織のセキュリティポリシーに基づいて、特定のオブジェクトにアクセスできるサブジェクトを決定します。アクセス制御はに基づいている可能性がありますか？
A. 組織における社会の役割。
B. 組織における個人の役割。
C. 組織における個人の役割に関連するグループダイナミクス。
D. 組織におけるマスタースレーブの役割に関連するグループダイナミクス。
Answer: B (メーッセージを残す**)**
アクセス制御モデルは、情報リソースへのユーザーアクセスに関するコンピューターおよび/またはネットワークシステムのルールを定義します。アクセス制御モデルは、機密性と整合性を提供し、監査証跡を通じて説明責任も提供します。監査証跡は、実行された操作の記録とともに、サブジェクトによるオブジェクトへのアクセスを文書化します。操作には、読み取り、書き込み、実行、および所有が含まれます。非随意アクセス制御は通常、役割ベースであり、組織内で個人が持つ役割（銀行の出納係、銀行モデルの融資担当者など）に基づいた承認決定によって一元管理されます。システムのセキュリティ管理者は、ユーザーの役割に基づいてシステム権限を付与および/または取り消します。このモデルは、人員の離職率が高い企業に適しています。

最新問題: **455**
次のうち、是正管理の例ではないものはどれですか？
A. OSのアップグレード
B. バックアップと復元
C. 緊急時対応計画
D. システム監視
Answer: D (メーッセージを残す**)**
質問のキーワードとしてNOTという単語が使用されています。修正制御ではない特定のオプションからセキュリティ制御を見つける必要があります。システム監視は検出制御であり、修正制御ではありません。試験では、さまざまなセキュリティ管理に関する以下の情報を知っておく必要があります
抑止制御抑止制御は、潜在的な攻撃者を思いとどまらせることを目的としています。アクセス制御は、潜在的な攻撃者が制御を回避しようとするのを防ぐのに十分であるという単純な事実によって、脅威や攻撃に対する抑止力として機能します。これは多くの場合、攻撃者が成功した場合の潜在的な報酬よりも制御を回避するために必要な労力がはるかに大きいため、または逆に、失敗した攻撃（または捕らえられた）の悪影響が成功の利点を上回っているためです。たとえば、ユーザー、サービス、またはアプリケーションの識別と認証、およびそれが意味するすべてを強制する

ことにより、攻撃者はインシデントとの関連を恐れるため、システムに関連するインシデントの可能性が大幅に減少します。特定のアクセスパスに対するコントロールがない場合、インシデントの数と潜在的な影響は無限になります。コントロールは、プロセスに監視を適用することにより、本質的にリスクへのエクスポージャーを減らします。この見落としは抑止力として機能し、起こりうる影響に直面して攻撃者の食欲を抑制します。抑止制御の最良の例は、従業員と、意図的に許可されていない機能を実行し、望ましくないイベントにつながる傾向があることによって示されます。ユーザーがシステムに認証して機能を実行することにより、ユーザーのアクティビティがログに記録されて監視されることをユーザーが理解し始めると、ユーザーがそのようなアクションを試みる可能性が低くなります。多くの脅威は脅威エージェントの匿名性に基づいており、それらのアクションとの識別および関連付けの可能性は、いかなる犠牲を払っても回避されます。アクセス制御が攻撃者による回避の主要なターゲットであるのは、この根本的な理由です。抑止力は、ユーザーが許可されていないことをした場合の潜在的な罰の形も取ります。たとえば、組織のポリシーで、許可されていないワイヤレスアクセスポイントを設置している従業員が解雇されると指定されている場合、ほとんどの従業員はワイヤレスアクセスポイントを設置できなくなります。

予防的管理予防的管理は、インシデントの発生を回避することを目的としています。予防的アクセス制御は、ユーザーが何らかのアクティビティや機能を実行できないようにします。予防的制御は、制御がオプションではなく、（簡単に）バイパスできないという点で抑止的制御とは異なります。抑止制御は、制御をバイパスした結果を危険にさらすよりも、制御に従う方が簡単であるという理論に基づいて機能します。言い換えれば、アクションの力はユーザー（または攻撃者）にあります。予防的制御はシステムに行動の力を与え、制御に従うことはオプションではありません。コントロールをバイパスする唯一の方法は、コントロールの実装に欠陥を見つけることです。

補償コントロール補償コントロールは、システムの既存の機能がポリシーの要件をサポートしていない場合に導入されます。補償コントロールは、技術的、手続き的、または管理的である可能性があります。既存のシステムは必要な制御をサポートしていない場合がありますが、既存の環境を補完し、制御のギャップを埋め、ポリシー要件を満たし、全体的なリスクを軽減できる他のテクノロジーまたはプロセスが存在する場合があります。たとえば、アクセス制御ポリシーでは、インターネットを介して実行する場合、認証プロセスを暗号化する必要があると規定されている場合があります。認証目的で暗号化をネイティブにサポートするようにアプリケーションを調整すると、コストがかかりすぎる可能性があります。暗号化プロトコルであるSecureSocketLayer（SSL）を採用し、認証プロセスの上に階層化して、ポリシーステートメントをサポートできます。他の例としては、システムの技術的限界を補い、トランザクションのセキュリティを確保するために特定のタスクを分離する機能を提供する職務分離環境があります。さらに、承認、監視、管理などの管理プロセスを使用して、アクセス制御環境のギャップを補うことができます。

探偵コントロール探偵コントロールは、何かが起こったときに警告し、インシデント後のタイムラインの最も早い時点です。アクセス制御は脅威に対する抑止力であり、最小限の特権を適用することで有害なインシデントを防ぐために積極的に利用できます。ただし、アクセス制御の検出機能は、アクセス環境の重要な可視性を提供し、組織がアクセス戦略と関連するセキュリティリスクを管理するのに役立ちます。前述のように、認証されたユーザーに提供される強力に管理さ

れたアクセス権限は、認証されたユーザーが持つ機能を制限することにより、企業の資産のリスクエクスポージャーを減らす機能を提供します。ただし、特権が提供された後にユーザーが実行できることを制御するためのオプションはほとんどありません。例えば、ユーザーにファイルへの書き込みアクセスが提供され、そのファイルが破損、変更、またはその他の方法で（意図的または意図せずに）悪影響を受けた場合、適用されたアクセス制御を使用すると、トランザクションを可視化できます。システムでの特権の識別、認証、許可、および使用に関するアクティビティをログに記録するための制御環境を確立できます。これは、エラーの発生、不正なアクションの実行の試みを検出するため、または提供された資格情報がいつ行使されたかを検証するために使用できます。検出デバイスとしてのロギングシステムは、許可されたユーザーによって実行されたアクション（成功と失敗の両方）とタスクの証拠を提供します。適用されたアクセス制御を使用すると、トランザクションを可視化できます。システムでの特権の識別、認証、許可、および使用に関するアクティビティをログに記録するための制御環境を確立できます。これは、エラーの発生、不正なアクションの実行の試みを検出するため、または提供された資格情報がいつ行使されたかを検証するために使用できます。検出デバイスとしてのロギングシステムは、許可されたユーザーによって実行されたアクション（成功と失敗の両方）とタスクの証拠を提供します。適用されたアクセス制御を使用すると、トランザクションを可視化できます。システムでの特権の識別、認証、許可、および使用に関するアクティビティをログに記録するための制御環境を確立できます。これは、エラーの発生、不正なアクションの実行の試みを検出するため、または提供された資格情報がいつ行使されたかを検証するために使用できます。検出デバイスとしてのロギングシステムは、許可されたユーザーによって実行されたアクション（成功と失敗の両方）とタスクの証拠を提供します。または、提供された資格情報がいつ行使されたかを検証します。検出デバイスとしてのロギングシステムは、許可されたユーザーによって実行されたアクション（成功と失敗の両方）とタスクの証拠を提供します。または、提供された資格情報がいつ行使されたかを検証します。検出デバイスとしてのロギングシステムは、許可されたユーザーによって実行されたアクション（成功と失敗の両方）とタスクの証拠を提供します。

是正措置セキュリティインシデントが発生した場合、セキュリティインフラストラクチャ内の要素に是正措置が必要になる場合があります。修正制御は、環境のセキュリティポスチャを変更して、欠陥を修正し、環境を安全な状態に戻すことを目的としたアクションです。セキュリティインシデントは、1つ以上の指示、抑止、予防、または補償の制御の失敗を示します。探偵コントロールがアラームまたは通知をトリガーした可能性がありますが、修正コントロールは、インシデントを追跡するために機能する必要があります。修正制御は、目前の特定の状況または対処する必要のある特定のセキュリティ障害に応じて、さまざまな形をとることができます。

回復制御セキュリティインシデントが発生した場合でも、一時的な補償制御を提供する場合でも、アクセス制御環境への変更は、正確に復元して通常の操作に戻す必要があります。アクセス制御、それらの適用性、ステータス、または管理に影響を与える可能性のあるいくつかの状況があります。イベントには、システムの停止、攻撃、プロジェクトの変更、技術的な要求、管理上のギャップ、および本格的な災害状況が含まれる可能性があります。たとえば、アプリケーションが正しくインストールまたは展開されていない場合、システムファイルに配置されたコントロールに悪影響を及ぼしたり、インストール時にデフォルトの管理者アカウントが無意識のうちに実装された

りする可能性があります。さらに、従業員は転勤、退職、または一時的な休暇をとることがあり、職務の分離に関するポリシー要件に影響を与える可能性があります。システムへの攻撃により、トロイの木馬プログラムが導入され、クレジットカード情報や財務データなどの個人ユーザー情報が公開される可能性があります。これらすべての場合において、望ましくない状況を可能な限り迅速に修正し、制御を通常の操作に戻す必要があります。
試験では、さまざまなセキュリティ管理に関する以下の情報を知っておく必要があります
抑止制御抑止制御は、潜在的な攻撃者を思いとどまらせることを目的としています。アクセス制御は、潜在的な攻撃者が制御を回避しようとするのを防ぐのに十分であるという単純な事実によって、脅威や攻撃に対する抑止力として機能します。これは多くの場合、攻撃者が成功した場合の潜在的な報酬よりも制御を回避するために必要な労力がはるかに大きいため、または逆に、失敗した攻撃 または捕らえられた)の悪影響が成功の利点を上回っているためです。たとえば、ユーザー、サービス、またはアプリケーションの識別と認証、およびそれが意味するすべてを強制することにより、攻撃者はインシデントとの関連を恐れるため、システムに関連するインシデントの可能性が大幅に減少します。特定のアクセスパスに対するコントロールがない場合、インシデントの数と潜在的な影響は無限になります。コントロールは、プロセスに監視を適用することにより、本質的にリスクへのエクスポージャーを減らします。この見落としは抑止力として機能し、起こりうる影響に直面して攻撃者の食欲を抑制します。抑止制御の最良の例は、従業員と、意図的に許可されていない機能を実行し、望ましくないイベントにつながる傾向があることによって示されます。ユーザーがシステムに認証して機能を実行することにより、ユーザーのアクティビティがログに記録されて監視されることをユーザーが理解し始めると、ユーザーがそのようなアクションを試みる可能性が低くなります。多くの脅威は脅威エージェントの匿名性に基づいており、それらのアクションとの識別および関連付けの可能性は、いかなる犠牲を払っても回避されます。アクセス制御が攻撃者による回避の主要なターゲットであるのは、この根本的な理由です。抑止力は、ユーザーが許可されていないことをした場合の潜在的な罰の形も取ります。たとえば、組織のポリシーで、許可されていないワイヤレスアクセスポイントを設置している従業員が解雇されると指定されている場合、ほとんどの従業員はワイヤレスアクセスポイントを設置できなくなります。
予防的管理予防的管理は、インシデントの発生を回避することを目的としています。予防的アクセス制御は、ユーザーが何らかのアクティビティや機能を実行できないようにします。予防的制御は、制御がオプションではなく、（簡単に）バイパスできないという点で抑止的制御とは異なります。抑止制御は、制御をバイパスした結果を危険にさらすよりも、制御に従う方が簡単であるという理論に基づいて機能します。言い換えれば、アクションの力はユーザー または攻撃者)にあります。予防的制御はシステムに行動の力を与え、制御に従うことはオプションではありません。コントロールをバイパスする唯一の方法は、コントロールの実装に欠陥を見つけることです。
補償コントロール補償コントロールは、システムの既存の機能がポリシーの要件をサポートしていない場合に導入されます。補償コントロールは、技術的、手続き的、または管理的である可能性があります。既存のシステムは必要な制御をサポートしていない場合がありますが、既存の環境を補完し、制御のギャップを埋め、ポリシー要件を満たし、全体的なリスクを軽減できる他のテクノロジーまたはプロセスが存在する場合があります。たとえば、アクセス制御ポリシーでは、イン

ターネットを介して実行する場合、認証プロセスを暗号化する必要があると規定されている場合があります。認証目的で暗号化をネイティブにサポートするようにアプリケーションを調整すると、コストがかかりすぎる可能性があります。暗号化プロトコルであるSecureSocketLayer（SSL）を採用し、認証プロセスの上に階層化して、ポリシーステートメントをサポートできます。他の例としては、システムの技術的限界を補い、トランザクションのセキュリティを確保するために特定のタスクを分離する機能を提供する職務分離環境があります。さらに、承認、監視、管理などの管理プロセスを使用して、アクセス制御環境のギャップを補うことができます。

探偵コントロール探偵コントロールは、何かが起こったときに警告し、インシデント後のタイムラインの最も早い時点です。アクセス制御は脅威に対する抑止力であり、最小限の特権を適用することで有害なインシデントを防ぐために積極的に利用できます。ただし、アクセス制御の検出機能は、アクセス環境の重要な可視性を提供し、組織がアクセス戦略と関連するセキュリティリスクを管理するのに役立ちます。

前述のように、認証されたユーザーに提供される強力に管理されたアクセス権限は、認証されたユーザーが持つ機能を制限することにより、企業の資産のリスクエクスポージャーを減らす機能を提供します。ただし、特権が提供された後にユーザーが実行できることを制御するためのオプションはほとんどありません。たとえば、ユーザーにファイルへの書き込みアクセスが提供され、そのファイルが破損、変更、またはその他の方法で（意図的または意図せずに）悪影響を受けた場合、適用されたアクセス制御を使用すると、トランザクションを可視化できます。システムでの特権の識別、認証、許可、および使用に関するアクティビティをログに記録するための制御環境を確立できます。これは、エラーの発生、不正なアクションの実行の試みを検出するために使用できます。または、提供された資格情報がいつ行使されたかを検証します。検出デバイスとしてのロギングシステムは、許可されたユーザーによって実行されたアクション（成功と失敗の両方）とタスクの証拠を提供します。

是正措置セキュリティインシデントが発生した場合、セキュリティインフラストラクチャ内の要素に是正措置が必要になる場合があります。修正制御は、環境のセキュリティポスチャを変更して、欠陥を修正し、環境を安全な状態に戻すことを目的としたアクションです。セキュリティインシデントは、1つ以上の指示、抑止、予防、または補償の制御の失敗を示します。探偵コントロールがアラームまたは通知をトリガーした可能性がありますが、修正コントロールは、インシデントを追跡するために機能する必要があります。修正制御は、目前の特定の状況または対処する必要のある特定のセキュリティ障害に応じて、さまざまな形をとることができます。

回復制御

セキュリティインシデントに直面した場合でも、

一時的な補償コントロールを提供し、正確に復元して通常に戻す必要があります

オペレーション。アクセス制御、その適用性、ステータスに影響を与える可能性のあるいくつかの状況があります。

または管理。

イベントには、システムの停止、攻撃、プロジェクトの変更、技術的な要求、管理などが含まれます。

ギャップ、そして本格的な災害状況。たとえば、アプリケーションが正しくインストールされていない場合や
デプロイすると、システムファイルに配置されたコントロールに悪影響を及ぼしたり、デフォルトが発生したりする可能性があります
インストール時に無意識のうちに管理アカウントが実装されました。
さらに、従業員は転勤、退職、または一時的な休暇をとることがあり、ポリシーに影響を与える可能性があります
職務の分離に関する要件。システムへの攻撃により、
トロイの木馬プログラムの埋め込み。次のような個人ユーザー情報を公開する可能性があります。
クレジットカード情報と財務データ。これらすべての場合において、望ましくない状況は
可能な限り迅速に修正され、コントロールは通常の操作に戻りました。
次の答えは正しくありません。
他の例は、修正管理に属しています。
この質問を作成するために、次の参照が使用されました。
CISAレビューマニュアル2014ページ番号44
と
公式ISC2CISSPガイド第3版ページ番号50および51

最新問題: **456**
次の火災抑制方法のうち、環境に優しく、データセンターに最も適しているのはどれですか？
A. 不活性ガス消火システム
B. ハロンガス消火システム
C. ドライパイプスプリンクラー
D. ウェットパイプスプリンクラー
Answer: A (メーッセージを残す**)**
ドライパイプとウェットパイプのスプリンクラーは水ベースであり、明らかな理由でデータセンターに設置することは絶対に避けてください。米国ではハロンガスが禁止されたため、不活性ガスの消火システムが残っています。
https://www.inertgasfiresystems.com/inert-gas-fire-suppression-systems/

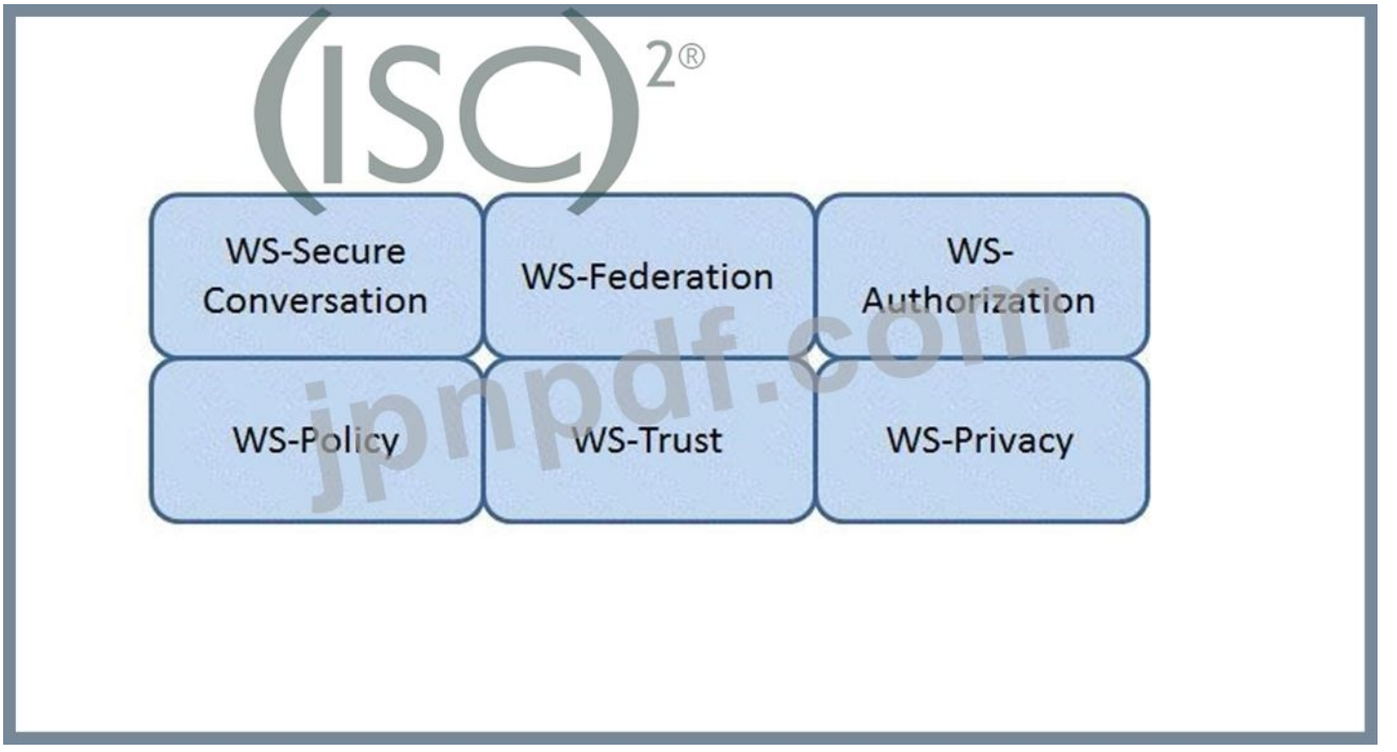
最新問題: **457**
次のうち、電子メールメッセージの信頼性と機密性を最もよく提供するのはどれですか？
A. 受信者の秘密鍵を使用してメッセージに署名し、送信者の公開鍵を使用してメッセージを暗号化する
B. 送信者の公開鍵を使用してメッセージに署名し、受信者の秘密鍵を使用してメッセージを暗号化する
C. 受信者の公開鍵を使用してメッセージに署名し、送信者の秘密鍵を使用してメッセージを暗号化する

D. 送信者の秘密鍵を使用してメッセージに署名し、受信者の公開鍵を使用してメッセージを暗号化する
Answer: D (メーッセージを残す**)**

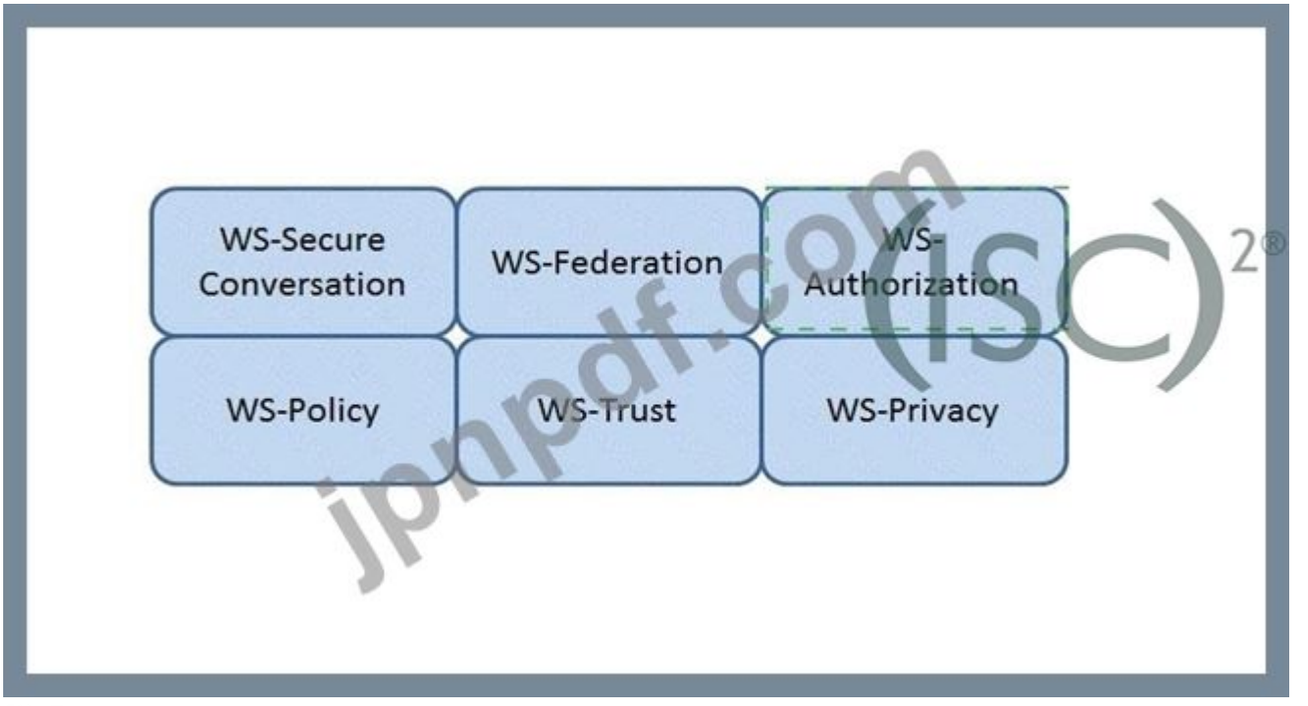
最新問題**: 458**
電子ボールティングは何を達成しますか？
A. 重要なファイルを保護します。
B. Redundant Array of Independent Disks（RAID）システムのフォールトトレランスを保証します
C. すべてのデータベースレコードをストライプ化します
D. ディザスタリカバリプロセス（DRP）を自動化します
Answer: (解答を表示する**)**
説明
セクション :セキュリティ運用

最新問題**: 459**
個人または企業が犯す可能性のある違反の1つは、ベンダーコードの逆コンパイルです。これは通常、その機能の複雑な詳細を理解することを期待して行われます。このタイプの非倫理的なエンジニアリングを最もよく表すものは何ですか？
A. リバースエンジニアリング
B. リバースエンジニアリング
C. リバースエンジニアリング
D. 転覆工学
Answer: B (メーッセージを残す**)**

最新問題**: 460**
どのWebサービスセキュリティ（WS-Security）仕様が、セキュリティトークンの管理とアクセスを許可するための基本的なポリシーを処理しますか？下の画像で正しい仕様をクリックしてください。



Answer:



説明

WS-承認

参照 :Java Webサービス：稼働中MartinKalin著228ページ

最新問題: **461**

生体認証システムでは、当初、真にポジティブな識別は人の身体的属性にのみ基づくことができることがすぐに明らかになりました。これにより、2つの質問に答える必要が生じました。

A. 人の性別と年齢は？

B. 体のどの部分を使用するか、そして実行可能な識別をどのように達成するか

C. 人の年齢と収入レベルは何歳でしたか
D. 人の声の調子と彼の習慣は何でしたか
Answer: (解答を表示する**)**
今日、高速で正確で信頼性が高く、ユーザーが受け入れられる生体認証システムの実装がすでに行われています。その目的のために、人の固有の身体的属性または行動が使用されます。From：TIPTON、Harold F.＆KRAUSE、MICKI、Information Security Management Handbook、4th Edition、Volume 1、Page 7

最新問題**: 462**
Bell-LaPadulaモデルは、次の項目のどれに対応していますか？
A. 被覆通信路
B. 安全な状態遷移の定義
C. 情報は高いものから低いものへと流れます
D. 主題とオブジェクトの作成と破壊
Answer: C (メーッセージを残す**)**
高から低への情報の流れは、Bell？LaPadulaモデルの*プロパティによって対処されます。これは、被験者が高レベルの分類から低レベルの分類にデータを書き込むことができないことを示しています。このプロパティは、閉じ込めプロパティまたは書き込みなしプロパティとも呼ばれます。
*回答 Covertchannels」では、隠密チャネルはモデルによってアドレス指定されていません。Bell-LaPadulaモデルは、通常のチャネルを介した情報の流れを処理し、意図しないパスを介した情報の秘密の通過には対応していません。 主題とオブジェクトの作成と破壊」と答える主題とオブジェクトの作成と破壊は、モデルによって扱われません。
*回答 セキュアな状態遷移の定義」とは、モデルが1つのセキュアな状態から別のセキュアな状態へのセキュアな遷移について説明しているという事実を指しますが、セキュアな遷移の定義を提供することはありません。

最新問題**: 463**
MACの下では、アクセス制御ポリシーで明示的に禁止されているアクセス権を誰が付与できますか？
A. 選択肢はありません。
B. すべてのユーザー。
C. 管理者のみ。
D. すべてのマネージャー。
Answer: (解答を表示する**)**
MACは、情報セキュリティ管理ハンドブックで次のように定義されています。必須の制御では、リソースの所有者ではなく管理者のみが、ポリシーに影響する、またはポリシーから派生する決定を行うことができます。リソースのカテゴリを変更できるのは管理者のみであり、アクセス制御ポリシーで明示的に禁止されているアクセス権を付与することはできません。

最新問題: **464**
積極的な調査のデータ収集プロセス中に遵守する必要がある最も重要な基準は何ですか？
A. 調査中に取られたすべてのアクションの概要
B. 管理過程の維持
C. 組織のセキュリティポリシーへの準拠
D. システムの画像をキャプチャする
Answer: D (メーッセージを残す**)**

最新問題: **465**
銀行の出納係のアクセス制御ポリシーは、次のうちどれを実装する例ですか？
A. ルールベースのポリシー
B. IDベースのポリシー
C. ユーザーベースのポリシー
D. 役割ベースのポリシー
Answer: D (メーッセージを残す**)**
説明/参照：
Explanation:
ロールベースのアクセス制御は、リソースへのアクセスがユーザーアカウントではなくジョブロールによって決定されるモデルです。この質問では、銀行の出納係が職務です。したがって、銀行の出納係のアクセス制御ポリシーは、役割ベースのポリシーです。
組織内では、さまざまな職務に対して役割が作成されます。特定の操作を実行するための権限は、特定の役割に割り当てられます。メンバーまたはスタッフ または他のシステムユーザー）には特定の役割が割り当てられ、それらの役割の割り当てを通じて、特定のコンピューターシステム機能を実行するためのコンピューター権限を取得します。ユーザーには直接権限が割り当てられるのではなく、自分の役割 または複数の役割）を通じてのみ権限を取得するため、個々のユーザー権限の管理は、ユーザーのアカウントに適切な役割を割り当てるだけで済みます。これにより、ユーザーの追加やユーザーの部門の変更などの一般的な操作が簡素化されます。
不正解：
A :ルールベースのアクセス制御では、一連のルールに基づいてリソースへのアクセスが許可または拒否されます。ルールには、グループのメンバーシップ、時刻などがあります。このモデルは、銀行の出納係などの職務を遂行する人にリソースへのアクセスを提供するためには使用されません。
B：銀行の出納係は職務であり、アイデンティティではありません。IDベースのポリシーでは、リソースへのアクセスは、ユーザーの役割ではなく、ユーザーのIDによって決定されます。
C :ユーザーベースのポリシーは、ユーザーが実行する役割ではなく、ユーザーが誰であるかによってリソースへのアクセスが決定されるIDベースのポリシーに似ています。
参照：
http://en.wikipedia.org/wiki/Role-based_access_control

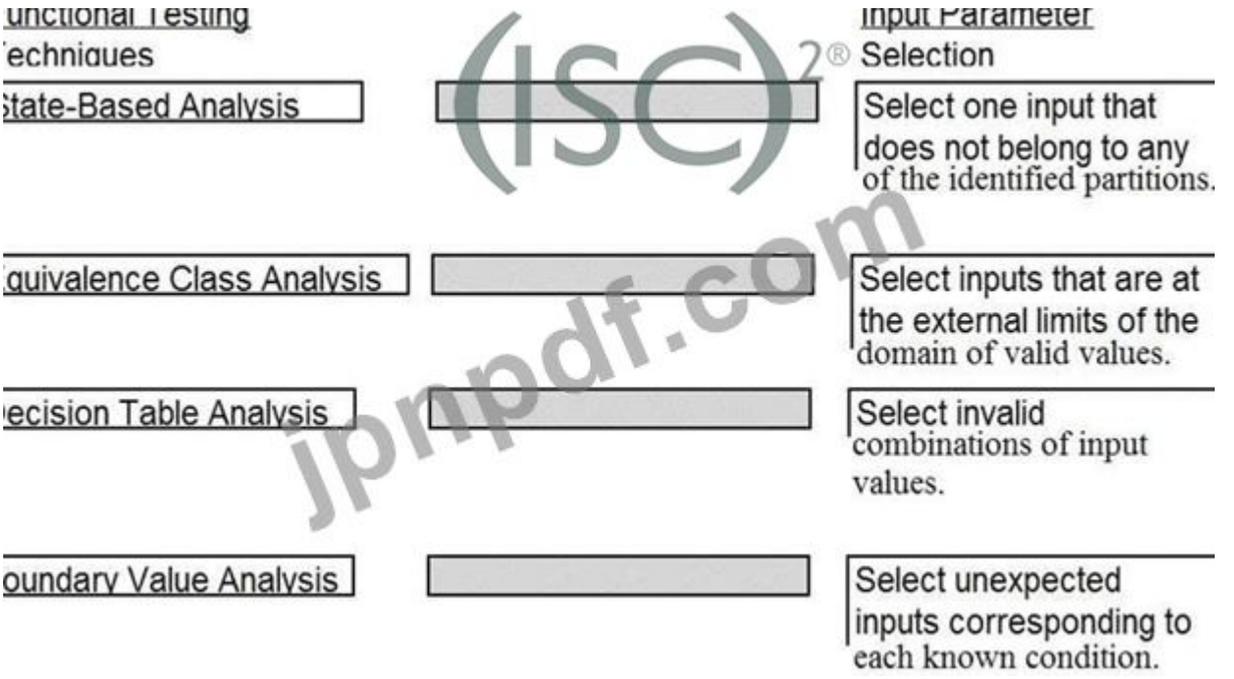
最新問題: **466**

以下の選択は、意図的に不適切な例ではありません
オペレーターの活動？
A. 不正なアクセスレベルを使用して情報の機密性を侵害する
B. 手動でトランザクションを入力するときにエラーが発生する
C. 会社のシステムを使用してポルノを保存する
D. 会社のシステムで民間事業を行う
Answer: (解答を表示する**)**
「トランザクションを手動で入力するときにエラーを発生させる」は、システムの整合性に対する脅威の例であることが最も確実ですが、意図的なアクティビティではなく、意図しない損失と見なされます。

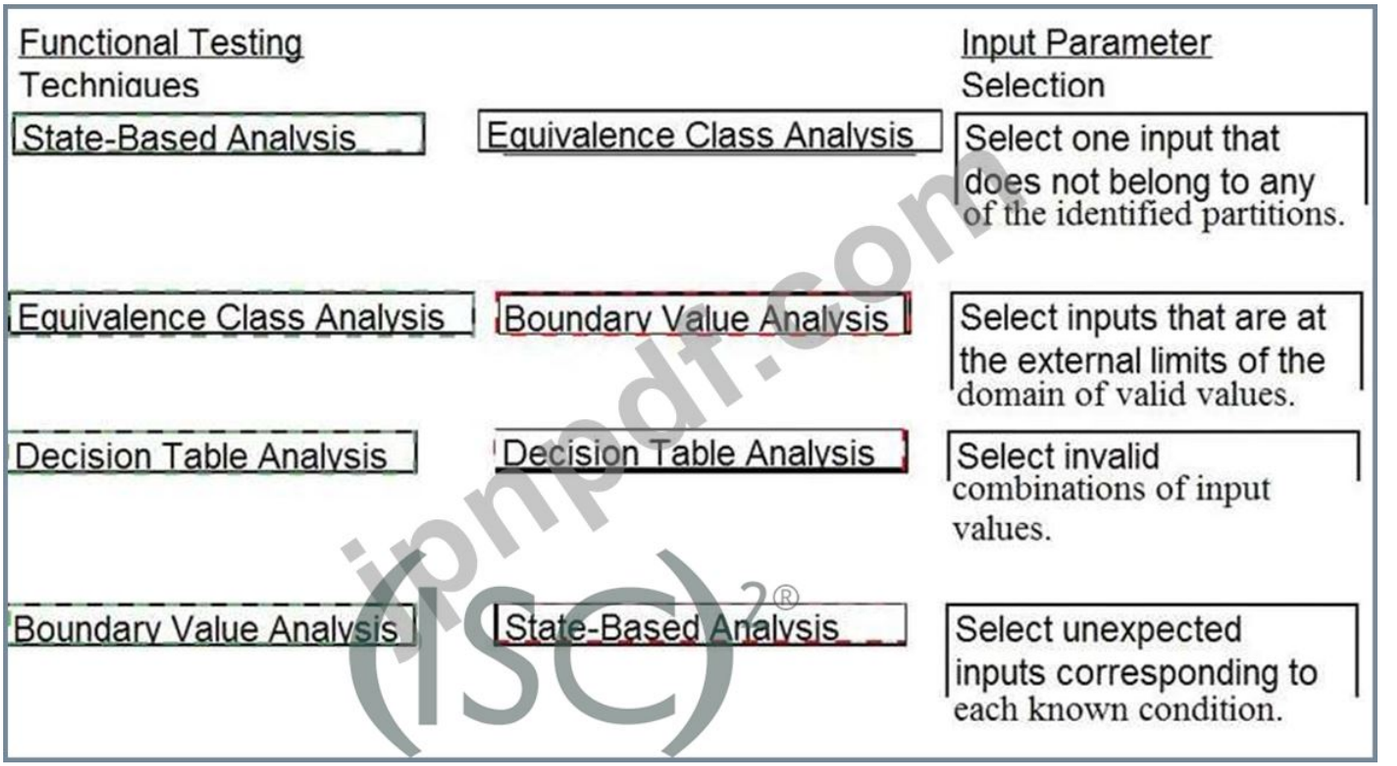
有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード**: Freepdfdumps**)

最新問題**: 467**
組織は、イントラネット上のファイルで従業員ポリシーを公開し、定期的に更新します。次のうち、主なセキュリティ上の懸念事項はどれですか？
A. 可用性
B. 整合性
C. 所有権
D. 守秘義務
Answer: B (メーッセージを残す**)**

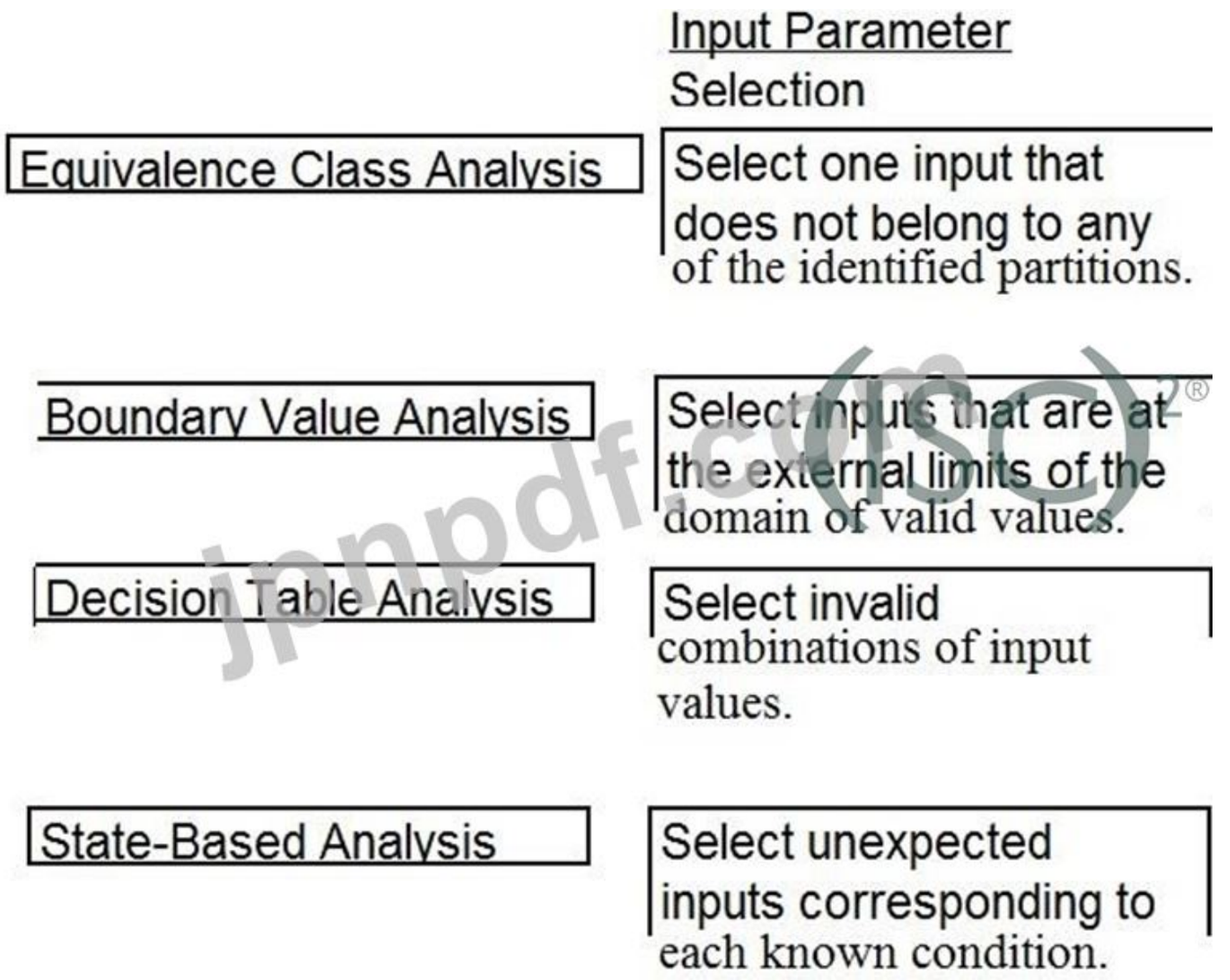
最新問題**: 468**
ソフトウェアセキュリティエンジニアは、ブラックボックスベースのテストプランを開発しています。このテストプランは、誤った入力や不正な入力、または予期しない操作エラーや状況に対するシステムの反応を測定します。左側の機能テスト手法を右側の正しい入力パラメーターと一致させます。


unctional Testing
echniques
Input Parameter
Selection
State-Based Analysis
Select one input that does not belong to any of the identified partitions.
quivalence Class Analysis
Select inputs that are at the external limits of the domain of valid values.
ecision Table Analysis
Select invalid combinations of input values.
oundary Value Analysis
Select unexpected inputs corresponding to each known condition.

Answer:


Functional Testing
Techniques
Input Parameter
Selection
State-Based Analysis
Equivalence Class Analysis
Select one input that does not belong to any of the identified partitions.
Equivalence Class Analysis
Boundary Value Analysis
Select inputs that are at the external limits of the domain of valid values.
Decision Table Analysis
Decision Table Analysis
Select invalid combinations of input values.
Boundary Value Analysis
State-Based Analysis
Select unexpected inputs corresponding to each known condition.

説明



jpnpdf.com (ISC)²®

最新問題: **469**

ホームオフィスや小規模オフィスに適したxDSLフレーバーのうち、アップストリームよりもダウンストリームで長距離の帯域幅を提供するのはどれですか？

A. VDSL

B. SDSL

C. ADSL

D. HDSL

Answer: (解答を表示する**)**

非対称デジタル加入者線（ADSL）は、アップストリーム（16～800Kb）よりもダウンストリーム（1～8 Mbps）でより多くの帯域幅を提供するように設計されています。

DSL（デジタル加入者線）は、家庭や企業からの通常の銅電話回線（POTS）を介したブロードバンドデータアクセスのためのモデムテクノロジです。xDSLは、ADSL（およびG.Lite）、HDSL、SDSL、IDSL、VDSLなどのすべてのタイプのDSLを総称します。これらは接続にのみ使用されるため、ラストマイル（またはファーストマイル）テクノロジーと呼ばれることもあります。電話交換局から自宅やオフィスへ、交換局間ではありません。

xDSLは、両方が既存の銅線電話回線で動作するという点でISDNに似ています。

（POTS）高度な変調方式を使用しており、どちらも中央電話局への短期間の実行が必要です。下の図：http ://computer.howstuffworks.com/vdsl3.htm
DSLスピードチャート
以下は不正解です。
単一回線デジタル加入者線（SDSL）は、片道2.3Mbpsの帯域幅を提供します。
高速デジタル加入者線（HDSL）は、片道1.544Mbpsの帯域幅を提供します。
非常に高速なデータレートのデジタル加入者線（VDSL）は、比較的短い距離（1000～4500フィート）で単一の銅線ツイストペアを介して最大52Mbpsのダウンストリームを配信できます。
この質問に使用される参照：
http://computer.howstuffworks.com/vdsl3.htm
と
http://www.javvin.com/protocolxDSL.html
と
KRUTZ、Ronald L.＆VINES、Russel D.、CISSP準備ガイド：10をマスターする
コンピュータセキュリティのドメイン、John Wiley＆Sons、2001年、第3章：電気通信とネットワークセキュリティ（115ページ）。

最新問題: **470**
次のうち、ホストベースの侵入検知システムの特徴ではないものはどれですか？
A. HIDSは大量のシステムリソースを消費しません
B. HIDSは、システムログ、プロセス、およびリソースを分析できます
C. HIDSは、システムへの不正な変更を探します
D. 異常なイベントが識別された場合、HIDSはシステム管理者に通知できます
Answer: A (メーッセージを残す)
HIDSは大量のシステムリソースを消費しないのが正しい選択です。HIDSは、特にイベント中に効果的に機能するために、CPUとシステムリソースを大量に消費する可能性があります。
他のすべての答えはHIDSの特徴です
HIDSは次のことができます。
-イベントログ、重要なシステムファイル、およびその他の監査可能なシステムリソースを精査します。
-不正な変更や疑わしい行動や活動のパターンを探す
-異常なイベントが発見されたときにアラートを送信できます
参照：
CISSPCBKの公式ガイド。197～198ページ。

最新問題: **471**
1996年、世界知的所有権機関（WIPO）が後援しました
参加国がデジタル著作権の取り扱いを標準化する条約。標準化の項目の1つは、著作物に含まれる著作権管理情報（CMI）の変更の禁止でした。CMIは次のとおりです。
A. ライセンスおよび所有権情報

B. 公開鍵のリスト
C. 暗号化アルゴリズム
D. 製品説明情報
Answer: (解答を表示する**)**
他の答えは気を散らすものです。米国をもたらしたWIPOデジタル著作権法は1998年のデジタル
ミレニアムでした
著作権法（DMCA）。回答dに対処することに加えて、
DMCAは、取引、製造、または販売を禁止します。
著作権保護メカニズムをバイパスすることを目的としています。また
無意識のうちにサポートしているインターネットサービスプロバイダー（ISP）に対応
購読者による著作物の投稿。ISPが
素材が著作権で保護されていることを通知された場合、ISPは
素材。さらに、投稿者が削除されたことを証明した場合
資料は合法的に使用されていたため、ISPは資料を復元する必要があります。
14営業日以内に著作権所有者に通知してください。
2001年にDMCAに関する2つの重要な判決が下されました。
判決には、DeCSSが含まれていました。これは、
表示を防ぐために使用されるコンテンツスクランブリングシステム（CSS）ソフトウェア
ライセンスのないプラットフォームでのDVDムービーディスクの使用。営業秘密の場合
[DVD-CCA v。Banner]、カリフォルニア州控訴裁判所は
インターネットにDeCSSを投稿した個人が下級裁判所の判決
CSSの企業秘密を明らかにしていた。控訴院は
DeCSSの投稿に関する差し止め命令を覆し、コードが
憲法修正第1条によって音声保護されています。
2番目のケース[UniversalCityv。Reimerdes]は、DMCAの迂回防止規則に対する最初の憲法上の異議申し立てでした。この事件には、ハッカー誌2600の発行者であるEricCorleyが関与していました。
雑誌。コーリーはDeCSSの状況をカバーし、
その報道は、彼の出版物のWebサイトにDeCSSを投稿しました。トライアル
と上訴裁判所は両方とも、投稿がDMCAに違反していると裁定しました
したがって、違法でした。この判決はDMCAを支持しました。現れる
将来的にはDMCAへの挑戦が増えるだろうと。

最新問題**: 472**
以下の選択は、保護プロファイル（PP）の最良の説明です。
コモンクライテリア（CC）で定義されているように？
A. 製品のセキュリティ要件の再利用可能な定義
B. セキュリティ要件コンポーネントの中間的な組み合わせ
C. 特定のITセキュリティ製品のセキュリティクレームのステートメント
D. 評価対象のIT製品またはシステム

Answer: A (メーッセージを残す)
コモンクライテリア（CC）は、次の2つの方法で使用されます。IT製品およびシステムのセキュリティ要件を説明する標準化された方法としてこれらの製品およびシステムのセキュリティ機能を評価するための適切な技術的基盤としてCCは、ITセキュリティを構築するための3つの有用な構成を定義します。要件：保護プロファイル（PP）、セキュリティターゲット（ST）、およびPackagE。PPは、一連のITセキュリティ製品のセキュリティニーズに関する実装に依存しないステートメントです。PPには一連のセキュリティ要件が含まれており、有用で効果的であることがわかっている製品のセキュリティ要件の再利用可能な定義となることを目的としています。APPは、消費者に特定のセキュリティニーズのセットを参照し、それらをメーカーに伝達する手段を提供し、それらのニーズに対する将来の製品評価を支援します。回答aは、セキュリティターゲット（ST）を定義します。STは、特定のITセキュリティ製品またはシステムに対するセキュリティクレームのステートメントです。STはPPの構造と類似していますが、製品固有の詳細情報を含む追加の要素があります。STは、製品またはシステムが提供するセキュリティに関するすべての関係者間の合意の基礎であり、したがって、そのセキュリティ評価の基礎です。*回答「セキュリティ要件コンポーネントの中間の組み合わせ」では、PackagEについて説明しています。パッケージは、セキュリティ要件コンポーネントの中間的な組み合わせです。このパッケージでは、セキュリティ目標のセットとして表現された、特定のニーズを満たす機能要件または保証要件のセットを表現できます。*回答「評価対象のIT製品またはシステム」評価対象（TOE）について説明します。TOEは、評価対象のIT製品またはシステムであり、そのセキュリティ特性は、対応するSTによって特定の用語で、またはPPによってより一般的な用語で記述されます。この評価は、認定された独立した研究所によって実施された厳密な分析とテストで構成されています。TOE評価の範囲は、評価保証レベル（EAL）およびSTで指定されたその他の要件によって設定されます。このプロセスの一部は、ST自体の評価であり、STが正しく、完全で、内部的に一貫性があり、TOE評価のベースラインとして使用できることを確認します。出典：コモンクライテリアプロジェクト。この評価は、認定された独立した研究所によって実施された厳密な分析とテストで構成されています。TOE評価の範囲は、評価保証レベル（EAL）およびSTで指定されたその他の要件によって設定されます。このプロセスの一部は、ST自体の評価であり、STが正しく、完全で、内部的に一貫性があり、TOE評価のベースラインとして使用できることを確認します。出典：コモンクライテリアプロジェクト。この評価は、認定された独立した研究所によって実施された厳密な分析とテストで構成されています。TOE評価の範囲は、評価保証レベル（EAL）およびSTで指定されたその他の要件によって設定されます。このプロセスの一部は、ST自体の評価であり、STが正しく、完全で、内部的に一貫性があり、TOE評価のベースラインとして使用できることを確認します。出典：コモンクライテリアプロジェクト。

最新問題: **473**
いくつかの異なるタイプの個別アクセスが存在するネットワーク情報システム（IS）を設計する場合、すべてのアクセス制御要件に確実に対応するために実行する必要がある最初のステップは何ですか？
A. ユーザープロファイルを作成します。

B. ユーザーアクセスマトリックスを作成します。
C. アクセス制御リスト（ACL）を作成します。
D. 役割ベースのアクセス制御（RBAC）リストを作成します。
Answer: B (メーッセージを残す**)**

最新問題**: 474**
ビジネスインパクト分析（BIA）は約
A. テクノロジー
B. 組織の使命を支援する
C. 十分な注意
D. リスク評価
Answer: B (メーッセージを残す**)**
ビジネスへの影響分析はテクノロジーに関するものではありません。それは使命を支援することについてです
組織の。
次の答えは正しくありません。
技術
十分な注意
リスクアセスメント
この質問を作成するために、次の参照が使用されました。
情報セキュリティ管理ハンドブック、Tipton＆AIによる第6版321ページ

最新問題**: 475**
Orange Bookによると、2種類のシステム保証とは何ですか？
A. 運用保証とアーキテクチャ保証。
B. 設計保証と実装保証。
C. アーキテクチャの保証と実装の保証。
D. 運用保証とライフサイクル保証。
Answer: D (メーッセージを残す**)**
オレンジの本で言及されている2種類の保証はありますか。
次の答えは正しくありません。
運用保証とアーキテクチャ保証。建築保証のために正しくありません
オレンジの本で言及されている種類の保証ではありません。
設計保証と実装保証。どちらもタイプではないため、正しくありません
オレンジの本で言及されている保証。
アーキテクチャの保証と実装の保証。どちらもタイプではないため、正しくありません
オレンジの本で言及されている保証。

最新問題**: 476**

着信データパケットの「状態」と「コンテキスト」を調べることにより、UDPベースのアプリケーションやUDPベースのアプリケーションなど、「コネクションレス」と見なされるプロトコルを追跡するのに役立ちます。
リモートプロシージャコール（RPC）。このタイプのファイアウォールシステムは？
A. 第1世代ファイアウォールシステム。
B. 第2世代ファイアウォールシステム。
C. 第3世代ファイアウォールシステム。
D. 第4世代ファイアウォールシステム。
Answer: (解答を表示する**)**
ステートフルインスペクションは、受信する情報だけでなく、受信する情報の動的接続と送信状態を認識して検査するように設計された第3世代ファイアウォールテクノロジーです。制御の決定は、通信情報、通信派生状態、アプリケーション派生状態、および情報操作を分析して利用することによって行われます。ファイアウォールのStatefullInspectionテクノロジーのいくつかの特徴は次のとおりです。
*
パケット内のすべてのレイヤーから情報をスキャンします。
*
FTPセッションの発信ポートコマンドなど、以前の通信から取得した状態情報を保存して、着信データ通信を検証できるようにします。
*
セッション状態データベースを使用して、コネクションレス型プロトコルの追跡サポートを提供します。
*
以前に認証されたユーザーなど、許可されたサービスに対してのみ、ファイアウォールを介した他のアプリケーションからの状態情報へのアクセスを許可します。
*
通信およびアプリケーションから派生した状態情報に基づいて、柔軟な式を評価および操作します。

最新問題: **477**
ファイアウォールを使用して
A. セキュリティポリシーを適用します。
B. データの機密性を保護します。
C. プロトコルリダイレクトから保護します。
D. セキュアネットワークインターフェイスのアドレス指定を適用します。
Answer: A (メーッセージを残す**)**
ファイアウォールは、会社のネットワークセキュリティポリシーをサポートおよび実施するデバイスです。-ションハリスオールインワンCISSP認定ガイド412ページ

最新問題: **478**
静的パスワードトークンについて正しいのは次のうちどれですか？
A. 所有者IDはトークンによって認証されます
B. 所有者がトークンによって認証されることはありません。
C. 所有者はシステムに対して自分自身を認証します。
D. トークンはトークンの所有者ではなくシステムを認証します。
Answer: A (メーッセージを残す**)**
トークンは、ユーザーのパスワードを提供する電子デバイスまたはカードです。トークンシステムを使用して、静的パスワードまたは動的パスワードのいずれかを提供できます。静的システムと動的システムには大きな違いがあります。静的システムは通常ユーザーをログインさせますが、動的システムはユーザーが自分でログインしなければならないことがよくあります。
静的パスワードトークン：
所有者IDはトークンによって認証されます。これは、所有者（通常は雇用主）にトークンを発行する人によって行われます。トークンの所有者は、 あなたが持っているもの」によって認証されるようになりました。トークンは、情報システムに対して所有者のIDを認証します。この発生の例は、従業員が自分のスマートカードを電子ロック上でスワイプして保管室にアクセスする場合です。
同期動的パスワードトークン：
このシステムは、静的トークンパスワードよりもはるかに複雑です。同期動的パスワードトークンは、メインシステムと同期される特定の時間間隔で新しいパスワードを生成します。パスワードは、ポケットベルや電卓に似た小さなデバイスで生成されます。これらのデバイスは、多くの場合、ユーザーのキーリングに取り付けることができます。各パスワードは特定の期間のみ有効です。間違った期間に間違ったパスワードを入力すると、認証が無効になります。時間的要因は、システムの故障である可能性もあります。システムの時計またはパスワードトークンデバイスが同期しなくなった場合、ユーザーはシステムへの認証に問題が発生する可能性があります。
非同期動的パスワードトークン：
クロック同期の問題は、非同期の動的パスワードトークンで解消されます。
このシステムは同期システムと同じプリンシパルで動作しますが、時間枠はありません。多くの大企業は、特に会社のVPN（仮想プライベートネットワーク）で自宅から仕事をする可能性のある従業員のためにこのシステムを使用しています。
チャレンジレスポンストークン：
これは興味深いシステムです。ユーザーには、ランダムまたは時間間隔で特別な チャレンジ」文字列が送信されます。ユーザーがこのチャレンジ文字列をトークンデバイスに入力すると、デバイスはチャレンジレスポンスを生成して応答します。次に、ユーザーはこの応答をシステムに入力し、それが正しい場合は認証されます。
この質問に使用される参照：
http://www.informit.com/guides/content.aspx?g=security&seqNum=146
と
KRUTZ、Ronald L.＆VINES、Russel D
CISSP準備ガイド :コンピュータセキュリティの10のドメインをマスターする、2001年、ジョン

Wiley＆Sons、37ページ

最新問題**: 479**
次のうち、ソーシャルエンジニアリングを最もよく定義しているのはどれですか？
A. 廃棄されたマニュアルや印刷物から情報を収集する
B. ソフトウェアの違法コピー
C. データの破壊または改ざん
D. 人のスキルを使用して専有情報を取得する
Answer: D (メーッセージを残す**)**
人のスキルを使用して専有情報を取得します。
*回答 「ソフトウェアの違法コピー」はソフトウェアの著作権侵害です
* 廃棄されたマニュアルと印刷物から情報を収集する」という回答はゴミ箱でのダイビングです。
*回答 「データの破壊または改ざん」は完全性の侵害です。

最新問題**: 480**
電子証拠の管理過程を詳述する証拠タグを作成するときに最も必要とされないのは次のうちどれですか？
A. 移動手段と移動手段。
B. 押収された情報の所有者に通知します。
C. 必要に応じて品質を含む、証拠の完全な説明。
D. 証拠を受け取ったのは誰か。
Answer: B (メーッセージを残す**)**
参考文献は、輸送が重要であることを示しています。
各証拠には、コレクターの日付、時刻、イニシャルを何らかの方法でマークする必要があります。
ケース番号が割り当てられている場合は...証拠の断片は、
コンテナとコンテナは同じ情報でマークする必要があります。コンテナは
証拠テープで封印され、可能であれば、壊れた封印ができるように、書き込みはテープにあるべきです
検出されます。-ションハリスオールインワンCISSP認定ガイドpg673
多くの場合、証人が法廷でオブジェクトを一意に識別することはできません。それらの中で
場合によっては、一連の証拠を確立する必要があります。これには、証拠を扱うすべての人が関与します-
それを最初に収集した警察、それを処理する証拠技術者、および
法廷でそれを使用する弁護士。証拠の場所は、から完全に文書化する必要があります
それが実際に同じであることを確認するためにそれが法廷に現れる瞬間までそれが集められた瞬間
アイテム。これには、証拠の徹底的なラベル付けと、誰がアクセスしたかを示す包括的なログが必要です。
特定の時期の証拠と、そのようなアクセスが必要な理由について。」593ページTittel：

CISSP学習ガイド。
証拠のライフサイクルは、証拠の収集と申請のプロセスをカバーしています。このライフサイクルには
次のコンポーネント：
発見と認識
保護
録音
コレクション
関連するすべてのストレージメディアを収集する
電源を切る前にハードディスクのイメージを作成します
画面を印刷する
機器の消磁は避けてください
身元
保存
磁気媒体を消去から保護します
適切な環境で保管する
交通手段
法廷でのプレゼンテーション
所有者への証拠の返却
ページ 309 Krutz :CISSP準備ガイド
証拠のライフサイクルには次のものが含まれます
*収集と識別
*保管、保存、および輸送
*法廷でのプレゼンテーション
*被害者または所有者に返還される
Pg 677ションハリス :オールインワンCISSP認定試験ガイド

最新問題: **481**
なぜバッファオーバーフローが発生するのですか？主な原因は何ですか？
A. バッファは非常に多くのデータしか保持できないため
B. アプリケーション内の不適切なパラメータチェックのため
C. 悪用しやすい弱点だから
D. システムメモリが不足しているため
Answer: (解答を表示する**)**
バッファオーバーフロー攻撃は、アプリケーション内の不適切なパラメータチェックを利用します。これはバッファオーバーフローの古典的な形式であり、プログラマーは、入力の長さがプログラム内のバッファーのサイズよりも小さいことを確認せずに、ユーザーが提供する入力を受け入れるために発生します。
バッファオーバーフローの問題は、ソフトウェア開発とプログラミングで最も古く、最も一般的な問題の1つであり、インタラクティブコンピューティングの導入にまでさかのぼります。これ

は、プログラムが割り当てられたメモリのバッファを、そのバッファが保持できるよりも多くのデータでいっぱいにした場合に発生する可能性があります。プログラムがバッファの終わりを超えて書き込みを開始すると、プログラムの実行パスを変更したり、オペレーティングシステム自体が使用する領域にデータを書き込んだりすることができます。これにより、プログラムまたはシステムの管理者権限を取得するために使用される可能性のある悪意のあるコードが挿入される可能性があります。
Gaurabが説明したように、それは非常に複雑になる可能性があります。入力時に、入力の長さをチェックしている場合でも、バッファサイズと照合する必要があります。データのエントリポイントがApplication1のBuffer1に格納され、後でApplication2内のBuffer2にコピーする場合を考えてみます。データの長さを、Buffer1と照合するだけでは、バッファオーバーフローが発生しないことは保証されません。Application2のBuffer2にあります。
試験に必要なコーディング知識のレベルに関するISC2の本からの少しの安心感：
CISSPは、エキスパートプログラマーである必要はなく、内部を知っている必要もありません。
FORTRANプログラミング言語のようなアプリケーションソフトウェアコードの開発の仕組み、または
Javaを使用してWebアプレットコードを開発する方法。CISSPが知っている必要さえありません
バッファオーバーフローエクスプロイトの主要な区分などの詳細なセキュリティ固有のコーディング慣行または
C言語でstrcpyよりもstr n cpyを好む理由（そのような知識はすべて、
もちろん、役に立ちました）。CISSPは、セキュリティが
このような開発に含まれるCISSPは、基本的な手順と概念を知っている必要があります
ソフトウェアプログラミングの設計と開発に関与します。つまり、
ソフトウェア開発プロセスを監視し、セキュリティが含まれていることを確認するCISSP、
CISSPは、プログラミング開発とセキュリティの基本的な概念を理解する必要があります
さまざまなアプリケーション開発プロセスの長所と短所。
以下は不正解です。
「バッファは非常に多くのデータしか保持できないため」は正しくありません。これは確かに真実ですが、最高ではありません
バッファの有限サイズは問題ではないので答えてください問題は
プログラマーは、入力をバッファーに移動する前に、入力のサイズをチェックしませんでした。
「悪用しやすい弱点だから」は正しくありません。この答えは時々真実ですが、
バッファオーバーフローの根本的な原因はプログラマーがしなかったことであるため、最良の答えではありません
ユーザー入力のサイズを確認してください。
「システムメモリが不足しているため」は正しくありません。これは、
バッファオーバーフロー。
この質問に使用される参照：
Hernandez CISSP、Steven（2012-12-21）。CISSP CBK、第3版の公式（ISC）2ガイド（（ISC）2 Press）Kindle Locations 13319-13323）。AuerbachPublications。キンドル版。

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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: **482**
次のうち、役割ベースのアクセス制御を正しく説明しているのはどれですか？
A. ユーザープロファイルグループにマップする方法で、エンタープライズ固有のセキュリティポリシーを指定して適用できます。
B. 組織の構造に対応する方法で、企業固有のセキュリティポリシーを指定して適用できます。
C. チケットシステムにマッピングする方法で、企業固有のセキュリティポリシーを指定して適用できます。
D. ACLにマッピングする方法で、エンタープライズ固有のセキュリティポリシーを指定して適用できます。
Answer: B (メーッセージを残す)
ロールベースのアクセス制御（RBAC）は、従来の随意アクセス制御（DAC）および強制アクセス制御（MAC）ポリシーの代替手段です。RBACの背後にある主な動機は、組織の構造に自然に対応する方法で企業固有のセキュリティポリシーを指定し、実施したいという願望です。従来、セキュリティを管理するには、組織のセキュリティポリシーを比較的低レベルの制御セット（通常はアクセス制御リスト）にマッピングする必要がありました。

最新問題: **483**
次のうち、ワイヤレスローカルエリアネットワーク（WLAN）の効果的な管理保証を提供するのはどれですか？
A. すべてのデフォルトパスワードが変更されたことを確認する
B. WLANクライアントデバイスとVPNコンセントレータの間に仮想プライベートネットワーク（VPN）トンネルを確立する
C. 許可されたアクセスポイント（AP）と接続デバイスのインベントリを維持する
D. 無線周波数を必要な最小範囲に設定する
Answer: C (メーッセージを残す)

最新問題: **484**
バイオメトリクスでは、個人の主張を検証するための1対1の検索
アイデンティティは呼ばれます：
A. 履歴書のレビューを監査します。
B. 説明責任。

C. 認証。
D. 集約。
Answer: C (メーッセージを残す**)**
正解は認証です。 取引の履歴のレビュー」に回答します。監査システムデータのレビューです、通常、事後に行われます。回答 説明責任」は個人に責任を負わせる
彼らの行動のために、そして答えdはより高い感度を得ています
感度の低い多数の情報からの情報。

最新問題**: 485**
Orange Bookによると、システムが個別のオペレーターとシステム管理者の役割をサポートすることを最初に要求するセキュリティレベルはどれですか？
A. A1
B. B1
C. B2
D. B3
Answer: C (メーッセージを残す**)**
B2セキュリティレベルでは、システムが個別のオペレーターとシステム管理者の役割をサポートする必要があります。
B3およびA1では、システムはセキュリティ関連の機能を実行するためにセキュリティ管理者の機能を明確に識別する必要があります。
出典 :KRUTZ、Ronald L.＆VINES、Russel D.、CISSP準備ガイド :マスタリング
コンピュータセキュリティの10のドメイン、John Wiley＆Sons、2001年、第6章：運用
セキュリティ 220ページ）。
また：
U.S。国防総省、Trusted Computer System Evaluation Criteria（Orange Book）、
DOD5200.28-STD。1985年12月（ここでも入手可能）。

最新問題**: 486**
ネットワーク上のすべてのホストは、syslog-ngを介してログコレクターにログを送信しています。ログコレクターは独自のファイアウォールの背後にあります。セキュリティの専門家は、ファイアウォールを通過するトラフィックの量が原因でファイアウォールに余分な負荷がかからないようにしたいと考えています。次のタイプのフィルタリングのうち、最も使用される可能性が高いのはどれですか？
A. URL（Uniform Resource Locator）フィルタリング
B. Webトラフィックフィルタリング
C. 静的パケットフィルタリング
D. 動的パケットフィルタリング
Answer: (解答を表示する**)**

最新問題**: 487**

プログラムを介してのみオブジェクトへのアクセスを導入するセキュリティモデルはどれですか？
A. ビバモデル
B. ベルラパドゥラモデル
C. クラークウィルソンモデル
D. 情報フローモデル
Answer: C (メーッセージを残す**)**
Clark-Wilsonモデルでは、サブジェクトはオブジェクトに直接アクセスできなくなりましたが、代わりにプログラム（整形式のトランザクション）を介してオブジェクトにアクセスする必要があります。
Clark-Wilson整合性モデルは、整合性を指定および分析するための基盤を提供します
コンピューティングシステムのポリシー。
このモデルは、主に情報の整合性の概念を形式化することに関係しています。情報
エラーまたはエラーによるシステム内のデータ項目の破損を防ぐことにより、整合性が維持されます
悪意。整合性ポリシーは、システム内のデータ項目をどのように保持するかを説明します
システムのある状態から次の状態まで有効であり、さまざまなプリンシパルの機能を指定します。
システム。モデルは、施行規則と認証規則を定義します。
Clark-Wilsonは、整合性が保たれているビジネスおよび業界のプロセスにより明確に適用できます。
情報コンテンツの割合は、分類のどのレベルでも最も重要です。
Clark-Wilsonモデルの整合性の目標：
許可されていないユーザーによる変更を防止します（これのみがBibaによって対処されます
モデル）。
職務の分離は、許可されたユーザーが不適切な変更を行うことを防ぎます。
整形式のトランザクション：内部および外部の一貫性を維持します。つまり、一連の操作です。
これは、ある一貫した状態から別の状態にデータを転送するために実行されます。
以下は不正解です。
ビバモデルが正しくありません。Bibaモデルは整合性に関係し、アクセスを制御します
サブジェクトのセキュリティレベルとオブジェクトのセキュリティレベルの比較に基づくオブジェクト。
Bell-LaPdaulaモデルが正しくありません。Bell-LaPaulaモデルは機密性に関係しています
対象のクリアランスレベルとの比較に基づいて、オブジェクトへのアクセスを制御します。
オブジェクトの分類レベル。
情報フローモデルが正しくありません。情報フローモデルは、オブジェクトが存在するラティスを使用します
はセキュリティクラスでラベル付けされており、情報は上向きまたは同じレベルで流れる可能性があります。です
フレームワークはベルラパドゥラモデルに似ています。

参照：
ISC2公式学習ガイド、325～327ページ
AIO3、pp.284-287
AIOv4セキュリティのアーキテクチャと設計（338～342ページ）
AIOv5セキュリティアーキテクチャと設計（341～344ページ）
ウィキペディア：https://en.wikipedia.org/wiki/Clark-Wilson_model

最新問題: **488**
次のうち、IPv6アドレスの正しい表記ではないものはどれですか？
A. 2001:0db8:0:0:0:0:1428:57ab
B. ABCD:EF01:2345:6789:
C. ABCD:EF01:2345:6789::1
D. 2001:DB8::8:800::417A
Answer: D (メーッセージを残す**)**
「:」はアドレスに1回しか表示されないため、これはIPv6アドレスの正しい表記ではありません。
「:」の使用は、16ビットのゼロの1つ以上のグループを示すショートカット表記です。
1は、特殊な表記を使用したループバックアドレスです。
参照：IPバージョン6アドレス指定アーキテクチャ
http://tools.ietf.org/html/rfc4291#section-2.1

最新問題: **489**
ポイントツーポイントプロトコル（PPP）がパケット形式を決定するために使用するのは次のうちどれですか？
A. レイヤー2トンネリングプロトコル（L2TP）
B. リンク制御プロトコル（LCP）
C. チャレンジハンドシェイク認証プロトコル（CHAP）
D. パケット転送プロトコル（PTP）
Answer: B (メーッセージを残す**)**
セクション：通信とネットワークセキュリティ

最新問題: **490**
次のうち、データ消去の形式ではないものはどれですか？
A. 残留磁気
B. パージ
C. クリア
D. 破壊
Answer: (解答を表示する**)**
クリアとは、データの上書きを指します
同じ組織で再利用することを目的としたメディア。パージとは
から削除することを目的としたメディアの消磁または上書き

組織。破壊とは、メディアを完全に破壊することです。

最新問題: **491**
システム管理オフィスは、次のルールを実装することを望んでいます。
-5年のスキルレベル3に指定された管理者
経験豊富で、システムのバックアップ、アップグレード、および
地方行政。
-スキルレベル5に指定され、10年の経験を持つ管理者は、システム管理に関連するすべてのアクションを実行できます。
この目標を達成するために実装する必要があるアクセス制御方法は次のうちどれですか？
A. 属性ベースのアクセス制御（ABAC）
B. 役割ベースのアクセス制御（RBAC）
C. 随意アクセス制御（DAC）
D. 強制アクセス制御（MAC）
Answer: (解答を表示する**)**

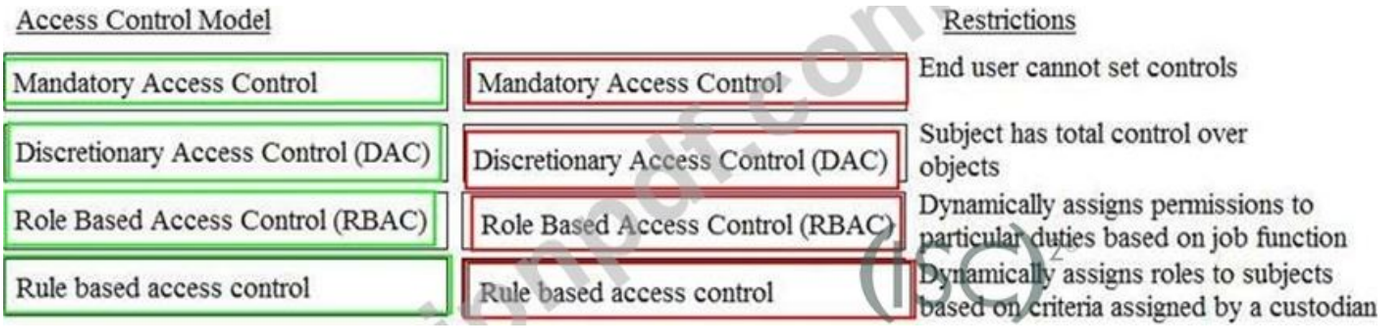
最新問題: **492**
次のうち、秘密チャネルとして使用できるのはどれですか？
A. 保管とタイミング。
B. ストレージと下位ビット。
C. ストレージと権限。
D. 保管と分類。
Answer: A (メーッセージを残す**)**
これらは適切な要素です。これら2つを使用して、被覆通信路を実現できます。ロービットは、隠れチャネルに関連する用語ではありません。権限は認証に関連しており、質問が望むことを達成しません。また、分類は正しい選択として選択できませんでした。
秘密チャネルとして使用できるものについては、CISSPの公式ドキュメントを確認してください。
盗聴のアクティブなバリエーションは、隠蔽チャネル盗聴と呼ばれ、隠された無許可のネットワーク接続を使用して無許可の情報を通信することで構成されます。隠密ストレージチャネルは、あるプロセスによってストレージに情報を書き込み、別のセキュリティから別のプロセスを使用して読み取ることによって動作しますレベル。秘密
タイミングチャネルは、独自のリソース使用を調整して別のプロセスの応答時間に影響を与えることにより、別のプロセスに情報を通知します。」Pg。101 Krutz :CISSP準備ガイド :ゴールドエディション

最新問題: **493**
組み合わせロックのセキュリティレベルを決定するものは何ですか？
A. ロックを開くために必要な組み合わせの複雑さ
B. 組み合わせをブルートフォースするのにかかる時間

C. 内部メカニズムに関連するバレルの数
D. 金属ロック材の硬度スコア
Answer: A (メーッセージを残す)
参照：
https://books.google.com.pk/books?id=RbihG-YALUkC&pg=PA976&lpg=PA976&dq=CISSP+determines+the

最新問題: **494**
アクセス制御モデルの名前を関連する制限と一致させます。
各アクセス制御モデルを右側の適切な制限アクセスにドラッグします。

Answer:



最新問題: **495**
パッチ管理プログラムを実装するときに最初に実行する手順は、次のうちどれですか。
A. システムインベントリを作成します。
B. パッチの自動展開を実行します。
C. 脆弱性の修正を優先します。
D. 脆弱性と脅威を監視します。
Answer: A (メーッセージを残す)

最新問題: **496**
オブジェクト指向プログラミングでは、1つのクラスのすべてのメソッドが
サブクラスに渡され、これは次のように呼ばれます。
A. 委任
B. 継承
C. 多重継承
D. 前向き連鎖

Answer: B (メーッセージを残す**)**
継承では、スーパークラスと呼ばれる1つのクラスのすべてのメソッドが、サブクラスによって継承されます。したがって、スーパークラスによって理解されるすべてのメッセージは、サブクラスによって理解されます。つまり、サブクラスはスーパークラスの動作を継承します。*前向き連鎖は気を散らすものであり、エキスパートシステムで使用されるデータ駆動型の推論を説明します。*複数の継承は、サブクラスが複数のスーパークラスの動作を継承する状況を表します。*回答の委任は、オブジェクト指向システムでの継承の代替手段です。委任を使用すると、オブジェクトが受信した要求を満たすメソッドを持たない場合、オブジェクトはその要求を別のオブジェクトに委任できます。

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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: **497**
コンテンツに依存する制御は、以下に基づいてアクセスを決定します。
A. オブジェクトの環境。
B. オブジェクトのビュー。
C. オブジェクトの所有者。
D. オブジェクトのデータ。
Answer: D (メーッセージを残す**)**
正解は 「オブジェクトのデータ」です。回答 「オブジェクトの環境」はコンテキスト依存の制御です。回答オブジェクトの所有者とオブジェクトのビューは気を散らすものです。

最新問題: **498**
6階建てのビルに情報処理施設を配置するのに最適なフロアは次のうちどれですか。
A. 3階
B. 地下
C. 1階
D. 6階
Answer: (解答を表示する**)**

最新問題: **499**
民間部門のデータ分類レベルによると、給与レベルと医療情報はどのように分類されますか？
A. 公開。
B. 内部使用のみ。

C. 制限付き。
D. 機密。
Answer: D (メーッセージを残す**)**
通常、ほとんどの組織で使用される情報分類には3〜4つのレベルがあります。機密情報：組織外に公開または開示された場合、組織に深刻な問題を引き起こす情報。たとえば、競争上の優位性を提供する情報（企業秘密、知的財産、研究デザインなど）は、技術的または経済的な成功にとって重要であるか、個人のプライバシーを保護する情報は機密情報と見なされます。情報には、給与情報、健康記録、信用情報、公式、技術設計、制限された規制情報、上級管理職の内部通信、またはビジネス戦略や計画が含まれる場合があります。これらは、トップシークレット、特権、個人、機密、または機密性の高いものと呼ばれることもあります。
次の回答は正しくありません。公開：会社、従業員、またはビジネスパートナーに危害を加えることを心配せずに一般に公開される可能性のある情報。特別な保護は必要ありません。このカテゴリの情報は、未分類と呼ばれることもあります。たとえば、会社の公開インターネットサイトに投稿された情報、公開された発表、マーケティング資料、カフェテリアメニュー、および開示されても会社に害を及ぼさない内部文書は、公開として分類されます。機密性についてはほとんど懸念がありませんが、整合性と可用性を考慮する必要があります。
内部使用のみ：社内で開示される可能性があるが、外部に開示された場合に会社に損害を与える可能性のある情報。顧客リスト、ベンダーの価格設定、組織のポリシー、標準と手順、内部組織の発表などの情報には、ベースラインのセキュリティ保護が必要ですが、機密情報としての保護レベルには達しません。言い換えれば、情報は社内で自由に使用できますが、社外での未承認の使用は害を及ぼす可能性があります。
制限付き：最大限の保護を必要とする情報、または権限のない担当者によって発見された場合に組織に取り返しのつかない損害を与える情報は、最高レベルの情報になります。
分類。組織内にはこのような情報はほとんどないかもしれませんが、
このレベルで分類されたデータには、利用可能なすべてのアクセス制御および保護メカニズムが必要です。
組織。このレベルで分類された情報が存在する場合でも、そのコピーはほとんどありません。
この質問に使用される参照：
Hernandez CISSP、Steven（2012-12-21）。CISSP CBK、第3版の公式（ISC）2ガイド（ISC）2 Press）Kindle Locations 952-976）。AuerbachPublications。キンドル版。

最新問題**: 500**
次のプロトコルのどれがセッション層（層5）で動作しますか？
A. RPC
B. IGMP
C. LPD
D. SPX
Answer: (解答を表示する**)**
説明/参照：
Explanation:

リモートプロシージャコール（RPC）は、OSIモデルのセッション層で機能します。
不正解：
B：ICMPはOSIモデルのネットワーク層で機能します。
C：LPD（Line Printer Daemon Protocol）は、アプリケーション層プロトコルです。
D：SPXはトランスポート層プロトコルです。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、New York、2013、p。524

最新問題: **501**
消火システムに関する次の説明のうち、正しいものはどれですか。
A. ハロンは、火の中の元素の化学反応を妨げるという点で非常に効果的であるため、エージェントに関する限り、今日最も一般的な選択肢です。
B. ガスマスクは、CO2システムの使用に対する効果的な保護を提供します。データセンター内の従業員を保護するために推奨されます。
C. CO2システムは、火災を維持するために必要な酸素供給を抑制するため、効果的ではありません。
D. 水ベースの消火器は、クラスC（電気）火災に効果的な消火方法ではありません。
Answer: (解答を表示する**)**
水ベースの消火器は、電気火災には絶対に使用しないでください。そうする場合、
おそらく、このような消火器を使って電気の火を消すのはこれが最後になるでしょう。
感電死。電気火災では、液体ベースの薬剤は避けてください。
CO2システムは、火災を持続させるために必要な酸素供給を抑制するため、効果的です。
酸素が除去されるので、それは潜在的に人々に致命的である可能性があり、ガスマスクは提供しません
CO2に対する保護。これらのシステムは、無人施設に適しています。
1987年のモントリオール議定書は、ハロンがオゾン層破壊に指定されていると述べています
物質と環境へのリスクのために、1994年1月1日に生産が停止されました。
ハロンシステムをまだ持っている会社はそれらを無毒で置き換えるように頼まれました
消火器。協定の名前はモントリオール議定書と呼ばれています。
ソーダ酸は、一般的な可燃物や液体には効果的な消火方法ですが、
電気火災。
ヒント：
国が持っているモントリオールで署名された協定の名前を覚えておいてください
ハロンの生産を停止することに合意しました、それは呼ばれます：モントリオール議定書
私の生徒は、火のクラスを思い出したいときに私のことを考えていると私に言いました。
それは私を少し怖がらせましたが、彼の説明は非常に理にかなっています、ここで彼は私の最初をどのように使用していますか
火のクラスを覚えておくための名前。私の名前はCLEMENTですが、彼はCLEMのみを使用しています。
部分：

C=一般的な可燃性
L=液体の火
E=電気火災
M=可燃性の金属
ハリソンからそれらを思い出す別の方法があります：
A-灰（一般的な可燃物）
B-バブル/ボイル（液体）
C-回路（電気）
D-金属。（覚えておいてください:)
この質問に使用される参照：
HARRIS、ション、オールインワンCISSP認定試験ガイド、McGraw-Hill / Osborne、2002年、章6：物理的セキュリティ（313ページ）。

最新問題: **502**
Orange Bookは、セキュリティシステムを分類するための4つの階層レベルについて説明しています。次のレベルのうち、必須の保護が必要なのはどれですか？
A. AとB。
B. BとC。
C. A、B、およびC。
D. BとD。
Answer: (解答を表示する**)**
説明/参照：
Explanation:
米国国防総省は、オペレーティングシステム、アプリケーション、およびさまざまな製品を評価するために使用される、信頼できるコンピュータシステム評価基準（TCSEC）を開発しました。これらの評価基準は、オレンジブックと呼ばれる本で公開されています。
TCSECは、保証レベルの階層区分に分割された分類システムを提供します。
A.検証済みの保護
B.必須の保護
C.裁量的保護
D.最小限のセキュリティ
分類Aは最高レベルの保証を表し、Dは最低レベルの保証を表します。
レベルBは、必須の保護が必要な最低レベルです。レベルAは、より高いレベルであるため、必須の保護も必要です。
不正解：
B :レベルCには必須の保護は必要ありません。レベルCは任意の保護です。
C :レベルCには必須の保護は必要ありません。レベルCは任意の保護です。
D :レベルDには必須の保護は必要ありません。レベルDは最小限のセキュリティです。
参照：

Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、New York、2013、pp.392-393

最新問題: **503**
2つの異なるキーがプレーンテキストメッセージを同じものに暗号化する場合
暗号文、この状況は次のように知られています。
A. 暗号解読。
B. 公開鍵暗号。
C. ハッシュ。
D. キークラスタリング。
Answer: D (メーッセージを残す**)**
正解は「キークラスタリング」です。回答「公開キー暗号化」は、公開キーと秘密キーを使用する暗号化システムのタイプを説明しています。答え暗号解読は暗号解読の芸術/科学です。回答ハッシュとは、可変長のメッセージを固定長のメッセージダイジェストに変換することです。

最新問題: **504**
National Computer Security Center（NCSC）は次のとおりです。
A. 情報セキュリティ意識向上トレーニングを提供し、機密であるが分類されていない情報を保護するための基準を開発する、米国商務省内の活動
B. 暗号化アルゴリズムと標準を開発するためのNSAとNISTの共同企業
C. 米国国立標準技術研究所（NIST）の一部門であり、暗号化機能の標準を発行し、それらを連邦情報処理標準（FIPS）として公開しています。
D. 調査を開始し、信頼できる情報システムの標準と基準を開発および公開する国家安全保障局（NSA）の支部
Answer: D (メーッセージを残す**)**
NCSCは、毎年恒例の全国情報システムセキュリティ会議を含む多くのチャネルを通じて、情報システムのセキュリティ意識と技術移転を促進しています。1981年に国防総省コンピュータセキュリティセンターとして設立され、1985年にNCScに社名が変更されました。情報システムのセキュリティ基準に照らして商用製品を評価するためのTrustedComputerEvaluationProgramRainbowシリーズを開発しました。したがって、他のすべての回答は、米国商務省の下にあるNISTを参照しているため、正しくありません。

最新問題: **505**
次のうち、コンピュータ調査の問題はどれですか？S
A. 調査の時間枠が短縮されます。
B. 専門家が支援を必要とする場合があります。
C. 情報は無形です。
D. 証拠は簡単に入手できます。
Answer: A,B,C (メーッセージを残す**)**

多くの場合、証拠は困難です
コンピュータ犯罪調査で取得します。

最新問題: **506**
随意アクセス制御（DAC）を使用するシステムは、次の攻撃のどれに対して脆弱ですか？
A. トロイの木馬
B. フリーキング
C. なりすまし
D. SYNフラッド
Answer: C (メーッセージを残す**)**
許可されたユーザーを装ってシステムにアクセスしようとする試み。なりすまし、なりすまし、または模倣と同義です。-Ronald Krutz CISSP PREPガイド（ゴールドエディション）921ページ「なりすまし有効な送信元および/または宛先IPアドレスとノード番号を誤ったものに置き換える行為。なりすまし攻撃-なりすましまたは変更されたパケットを含む攻撃。」--Ed Tittle CISSP学習ガイド（Sybex）

最新問題: **507**
ネットワークセキュリティ評価の完了後、次のうちどれが最もよく示されることができますか？
A. コントロールの有効性を正確に測定できます
B. ネットワークは業界標準に準拠しています
C. パッチが適用されていないすべての脆弱性が特定されました
D. ネットワークの侵入テストは失敗します
Answer: (解答を表示する**)**

最新問題: **508**
次のうち、緊急事態に備えて従業員を準備するための意識向上およびトレーニング計画の最も重要な部分はどれですか？
A. 企業のウェブサイトで企業の事業継続と災害復旧計画を公開する
B. 復旧に直接的な役割を果たす人々のために事業継続と災害復旧トレーニングを実施する
C. 一般の従業員が情報を入手するための緊急連絡先を確立する
D. さまざまな対象者向けのビジネス継続性および災害復旧トレーニングプログラムの設計
Answer: D (メーッセージを残す**)**

最新問題: **509**
悪用可能な欠陥を見つけて標的にするために、組織はどのタイプのテストを実行しますか？
A. 浸透
B. システム
C. パフォーマンス
D. 脆弱性
Answer: (解答を表示する**)**

セクション :セキュリティの評価とテスト

最新問題: **510**
アクセス制御の主なカテゴリには、次のものは含まれません。
A. 管理アクセス制御
B. 論理アクセス制御
C. ランダムアクセス制御
D. 物理的アクセス制御
Answer: (解答を表示する**)**
アクセス制御にはいくつかの異なるカテゴリがあります。主なカテゴリは次のとおりです。--物理アクセス制御管理アクセス制御論理アクセス制御データアクセス制御

最新問題: **511**
データへのアクセスを適切に分類して保護するために、セキュリティの専門家が組織の資産のセキュリティを評価する際に最初に実行する必要があるアクションは何ですか？
A. 組織内でデータにアクセスする方法を決定します。
B. データとシステムへのアクセスレベルを決定します。
C. さまざまな環境に実装されているさまざまなデータ分類モデルを確認します。
D. 機密データが暗号化で保護されているかどうかを確認します。
Answer: A (メーッセージを残す**)**

有効な **CISSP** 問題集は GoShiken.com が提供された合格しやすい CISSP 試験問題集！GoShiken.com が最新の **CISSP** 試験問題集を提供しています。GoShiken.com CISSP 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CISSP 問題集をゲットする人はこちら: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**153330%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: **512**
次のうち、非対称鍵アルゴリズムではないものはどれですか？
A. RSA
B. 楕円曲線暗号システム（ECC）
C. El Gamal
D. データ暗号化システム（DES）
Answer: (解答を表示する**)**
データ暗号化規格（DES）は、対称鍵アルゴリズムです。もともとIBMによってプロジェクト名Luciferで開発された、この128ビットアルゴリズムは1974年にNISTによって受け入れられましたが、キーサイズは56ビットとパリティ用の8ビットに縮小されました。それはどういうわけか1977年に国家暗号規格になり、米国規格協会（ANSI）規格になりました。

1978年。DESは後にNISTによってAdvancedEncryptionStandard（AES）に置き換えられました。他のすべて
オプションは非対称アルゴリズムです。
出典：HARRIS、ション、オールインワンCISSP認定試験ガイド、McGraw-Hill / Osborne、2002年、第8章：暗号化525ページ）。
参照：DES：http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

最新問題: **513**
どのタイプのディザスタリカバリプラン（DRP）テストが、最も運用上のリスクを伴いますか？
A. ウォークスルー
B. 卓上
C. 並列
D. カットオーバー
Answer: (解答を表示する)

最新問題: **514**
同じ平文から同じ暗号文を生成する2つの異なるキーのインスタンスとして何を定義できますか？
A. キーの衝突
B. キークラスタリング
C. ハッシュ
D. 暗号文の衝突
Answer: (解答を表示する)
キークラスタリングは、プレーンテキストメッセージが同じ変換アルゴリズムを使用して同一の暗号文メッセージを生成するが、キーが異なる場合に発生します。出典：KRUTZ、Ronald L.＆VINES、Russel D.、CISSP Prep Guide：Mastering the Ten Domains of Computer Security、John Wiley＆Sons、2001年、第4章：暗号化130ページ）。

最新問題: **515**
フェデレーションIDソリューションでクラウドベースのディレクトリを作成するための前提条件となるテクノロジーはどれですか？
A. 通知ツール
B. メッセージキューツール
C. セキュリティトークンツール
D. 同期ツール
Answer: (解答を表示する)
セクション：ソフトウェア開発のセキュリティ

最新問題: **516**
多くの場合、どのRAIDレベルが1対1のディスク対ディスクの比率を実装しますか？

A. RAIDレベル1
B. RAIDレベル0
C. RAIDレベル2
D. RAIDレベル5
Answer: A (メーッセージを残す**)**
RAIDレベル1は、多くの場合、1対1のディスクとディスクの比率で実装されます。
出典 :KRUTZ、Ronald L.＆VINES、Russel D.、CISSP準備ガイド :Mastering the Ten Domains of Computer Security、2001年、John Wiley＆Sons、65ページ。
関連項目 :ハリス、ション、オールインワンCISSP認定試験ガイド、マグロウヒル/オズボーン、2002年、第7章：電気通信とネットワークセキュリティ 480ページ）。
参照：「このレベルは、あるディスクから別のディスクへのすべてのディスク書き込みを複製して、2つの同一のディスクを作成します
ドライブ。この手法は、データミラーリングとも呼ばれます。このレベルで冗長性が提供されます」
出典 :CISSPCBKの公式ISC2ガイド。p。657
RAIDレベル0- 「パリティ情報を使用せずに、複数のディスクにまたがってファイルをストライプで書き込みます。
この手法により、ディスクの読み取りと書き込みを高速化できます。ただし、パリティ情報がない場合は、
ハードドライブの障害から回復することはできません。」出典 :CISSPCBKの公式ISC2ガイド。p。657
RAIDレベル2- 「データは、この手法を使用してビットレベルで複数のディスクに分散されます。冗長性情報は、ハードドライブおよびエラー訂正メモリモジュールで使用されるのと同じ手法であるハンマーエラー訂正コードを使用して計算されます。」出典 :CISSPCBKの公式ISC2ガイド p.657-658
RAIDレベル5- 「このレベルを実装するには、3つ以上のドライブが必要です。データとパリティ情報はすべてのドライブでストライプ化されます。このレベルは最も一般的であり、1つのドライブの損失に耐えることができます。」出典 :CISSPCBKの公式ISC2ガイドp。658

最新問題**: 517**
次のうち、ボーダーゲートウェイプロトコル（BGP）の目的を最もよく表しているのはどれですか？
A. ルーティング情報プロトコル（RIP）バージョン2アドバタイズメントを隣接するレイヤー3デバイスに提供します。
B. 自律システム間の効率的なネットワークパスのリストを維持します。
C. クラウド対応アプリケーションにファイアウォールサービスを提供します。
D. インターネットルーター間のネットワークパスのリストを維持します。
Answer: (解答を表示する**)**

最新問題: **518**
次のうち、リモートアクセスのセキュリティ目標ではないものはどれですか？
A. ユーザーとシステムの信頼性の高い認証
B. 機密データの保護
C. システムおよびネットワークリソースへのアクセス制御を管理しやすい
D. リモートユーザーの自動ログイン
Answer: D (メーッセージを残す**)**
リモートユーザーの自動ログイン機能は、弱い認証を意味しますが、
したがって、確かにセキュリティの目標ではありません。
出典 :TIPTON、Harold F.&KRAUSE、Micki、Information Security Management Handbook、4th エディション、ボリューム2、2001、CRC Press、第5章 :セキュアリモートアクセスの概要（ページ 100）。

最新問題: **519**
クラウド環境への違反に続いて、どれが最大のインポートになりますか？
A. 不十分なネットワーク分離
B. すべてのVMに同じ論理ユニット番号（LUN）が使用されます
C. 仮想マシン（VM）の不十分な強化
D. ハイパーバイザーホストの焼き付けが不十分
Answer: A (メーッセージを残す**)**

最新問題: **520**
セキュリティ計画の準備手順には、次のうちどれを除いて、次のすべてが含まれますか？
A. 目標を設定します。
B. 計画の前提条件を一覧表示します。
C. セキュリティ監査機能を確立します。
D. 代替の行動方針を決定する
Answer: C (メーッセージを残す**)**
説明/参照：
Explanation:
セキュリティポリシーは、組織内でセキュリティが果たす役割を指示する、上級管理職（または選択されたポリシー委員会または委員会）によって作成された全体的な一般的なステートメントです。セキュリティポリシーは、組織ポリシー、問題固有のポリシー、またはシステム固有のポリシーにすることができます。組織のセキュリティポリシーでは、管理者はセキュリティプログラムの設定方法を確立し、プログラムの目標を設定し、責任を割り当て、セキュリティの戦略的および戦術的価値を示し、施行の実行方法を概説します。
セキュリティ計画には、目標の設定、前提条件の一覧表示、および代替の行動方針の決定を含める必要があります。

セキュリティ計画には、セキュリティ監査機能の確立は含まれていません。セキュリティの監査は、セキュリティ計画に記載されているように実施されたセキュリティ対策が効果的であることを確認するために実行されます。
不正解：
A :セキュリティ計画には、目標の設定を含める必要があります。
B :セキュリティ計画には、リストの前提条件を含める必要があります。
D :セキュリティ計画には、代替の行動方針の決定を含める必要があります。
参照：
Harris、Shon、All In One CISSP Exam Guide、6th Edition、McGraw-Hill、New York、2013、p。102

最新問題: **521**
チャネル分析、信頼できる施設管理、および信頼できる
回復はTCSECレインボーシリーズのどの本の一部ですか？
A. レッドブック
B. ダークグリーンブック
C. オレンジブック
D. グリーンブック
Answer: (解答を表示する**)**
正解はオレンジブックです。
*レッドブックに答えるのは信頼できるネットワークです
ネットワーク要件の解釈（TNI）の要約（説明
電気通信およびネットワークセキュリティドメイン内）。
* Green Bookは、国防総省（DoD）のパスワード管理ガイドラインです。
* Dark Green Bookは、自動化されたデータの残りを理解するためのガイドです。
情報システム。

Valid CISSP Dumps shared by GoShiken.com for Helping Passing CISSP Exam! GoShiken.com now offer the **newest CISSP exam dumps**, the GoShiken.com CISSP exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com CISSP dumps with Test Engine here: https://www.goshiken.com/ISC/CISSP-mondaishu.html (**1533** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)