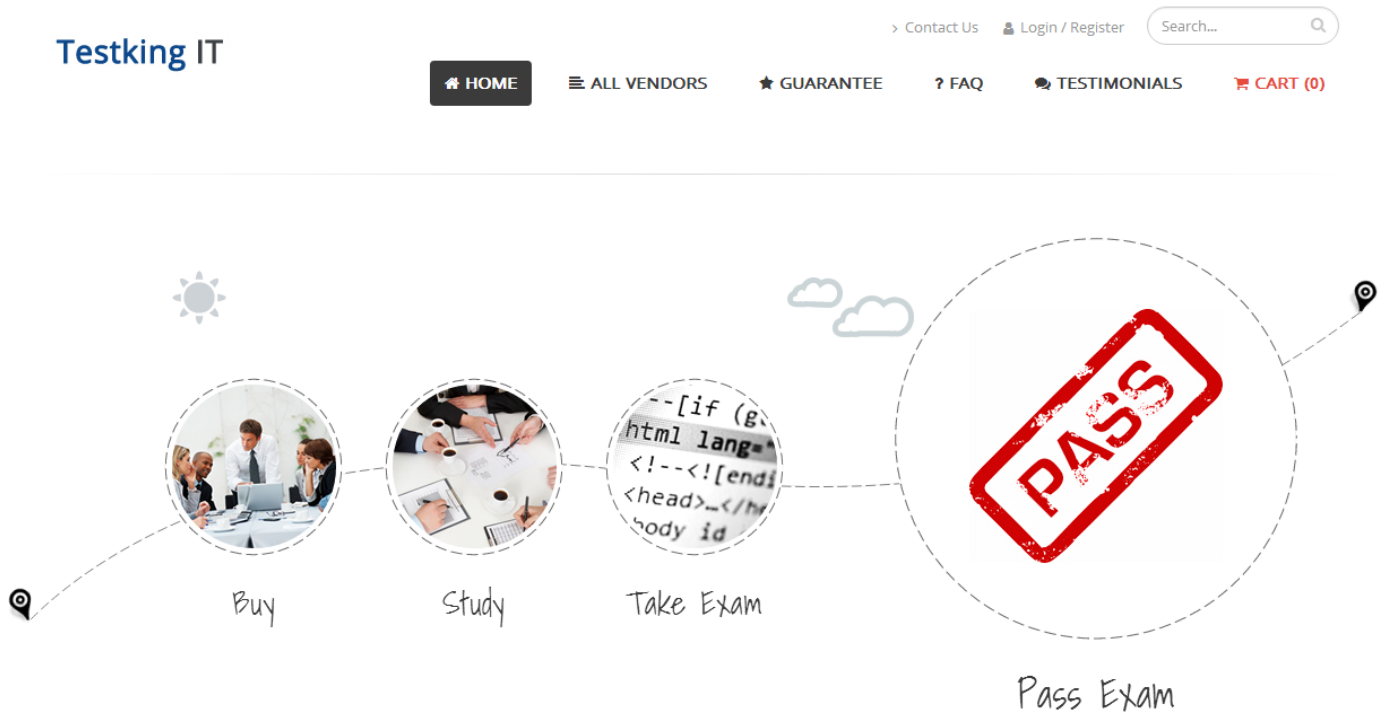
TestkingIT



Try **Desktop Test Engine** before you buy

We're not the only ones **happy** about TestKingsIT Practice Material ...

48236+ customers in 100+ countries use TestKingsIT Test Engine. Meet our customers.

iMessenger VOREED GetCustom JET ORANGE iCompany Paradoxx

http://www.testkingit.com/

Latest practice material - Exam Cram - TestKingIT

Exam : **SSCP-JPN**

Title : System Security Certified Practitioner (SSCP日本語版)

Vendor : ISC

Version : DEMO

QUESTION NO: 1
次のうち、単一のコンピュータ システムで多数のプロセッサ
ユニットを使用して、アプリケーション環境でのシステムのパフォーマンスを同種の単一のプロセッサのパフォーマンスよりも向上させる手法を説明しているのはどれですか?
A. マルチタスク
B. マルチプログラミング
C. パイプライン
D. マルチプロセッシング
Answer: D
Explanation:
Multiprocessing is an organizational technique in which a number of processor units are employed in a single computer system to increase the performance of the system in its application environment above the performance of a single processor of the same kind. In order to cooperate on a single application or class of applications, the processors share a common resource. Usually this resource is primary memory, and the multiprocessor is called a primary memory multiprocessor. A system in which each processor has a private (local) main memory and shares secondary (global) memory with the others is a secondary memory multiprocessor, sometimes called a multicomputer system because of the looser coupling between processors.
The more common multiprocessor systems incorporate only processors of the same type and performance and thus are called homogeneous multiprocessors; however, heterogeneous multiprocessors are also employed. A special case is the attached processor, in which a second processor module is attached to a first processor in a closely coupled fashion so that the first can perform input/output and operating system functions, enabling the attached processor to concentrate on the application workload.
The following were incorrect answers:
Multiprogramming: The interleaved execution of two or more programs by a computer, in which the central processing unit executes a few instructions from each program in succession.
Multitasking: The concurrent operation by one central processing unit of two or more processes.
Pipelining: A procedure for processing instructions in a computer program more rapidly, in which each instruction is divided into numerous small stages, and a population of instructions are in various stages at any given time. One instruction does not have to wait for the previous one to complete all of the stages before it gets into the pipeline. It would be similiar to an assembly chain in the real world.

QUESTION NO: 2
通信を容易にするためにネットワーク
デバイスを編成する方法として定義されるものは何ですか?
A. LAN 伝送方式
B. LAN トポロジー
C. LAN 伝送プロトコル
D. LAN メディア アクセス方式

Answer: C
Explanation:
Bridges are simple, protocol-dependent networking devices that are used to connect two or more homogeneous LANs to form an extended LAN.
A bridge does not change the contents of the frame being transmitted but acts as a relay.
A gateway is designed to reduce the problems of interfacing any combination of local networks that employ different level protocols or local and long-haul networks.
A router connects two networks or network segments and may use IP to route messages.
Firewalls are methods of protecting a network against security threats from other systems or networks by centralizing and controlling access to the protected network segment.

QUESTION NO: 3
RSAアルゴリズムは、暗号化の基礎としてどの数学的概念を使用していますか?
A. ジオメトリ
B. 16ラウンド暗号
C.PI (3.14159...)
D. 2 つの大きな素数
Answer: C

QUESTION NO: 4
ハイジャックを防ぐのに最も適した認証技術はどれですか?
A. 静的認証
B. 継続認証
C. 堅牢な認証
D. 強力な認証
Answer: B
Explanation:
A continuous authentication provides protection against impostors who can see, alter, and insert information passed between the claimant and verifier even after the claimant/verifier authentication is complete. This is the best protection against hijacking. Static authentication is the type of authentication provided by traditional password schemes and the strength of the authentication is highly dependent on the difficulty of guessing passwords. The robust authentication mechanism relies on dynamic authentication data that changes with each authenticated session between a claimant and a verifier, and it does not protect against hijacking.
Strong authentication refers to a two-factor authentication (like something a user knows and something a user is).

QUESTION NO: 5
脅威によって悪用され、情報システムやネットワークに損害を与える可能性のある脆弱性や保護手段の欠如は、?と呼ばれます。
A. 脆弱性
B. リスク
C. 脅威

D. オーバーフロー

Answer: C

Explanation:

Security is generally defined as the freedom from danger or as the condition of safety. Computer security, specifically, is the protection of data in a system against unauthorized disclosure, modification, or destruction and protection of the computer system itself against unauthorized use, modification, or denial of service. Because certain computer security controls inhibit productivity, security is typically a compromise toward which security practitioners, system users, and system operations and administrative personnel work to achieve a satisfactory balance between security and productivity.

Controls for providing information security can be physical, technical, or administrative. These three categories of controls can be further classified as either preventive or detective. Preventive controls attempt to avoid the occurrence of unwanted events, whereas detective controls attempt to identify unwanted events after they have occurred. Preventive controls inhibit the free use of computing resources and therefore can be applied only to the degree that the users are willing to accept. Effective security awareness programs can help increase users' level of tolerance for preventive controls by helping them understand how such controls enable them to trust their computing systems. Common detective controls include audit trails, intrusion detection methods, and checksums.

Three other types of controls supplement preventive and detective controls. They are usually described as deterrent, corrective, and recovery.

Deterrent controls are intended to discourage individuals from intentionally violating information security policies or procedures. These usually take the form of constraints that make it difficult or undesirable to perform unauthorized activities or threats of consequences that influence a potential intruder to not violate security (e.g., threats ranging from embarrassment to severe punishment).

Corrective controls either remedy the circumstances that allowed the unauthorized activity or return conditions to what they were before the violation. Execution of corrective controls could result in changes to existing physical, technical, and administrative controls. Recovery controls restore lost computing resources or capabilities and help the organization recover monetary losses caused by a security violation.

Deterrent, corrective, and recovery controls are considered to be special cases within the major categories of physical, technical, and administrative controls; they do not clearly belong in either preventive or detective categories. For example, it could be argued that deterrence is a form of prevention because it can cause an intruder to turn away; however, deterrence also involves detecting violations, which may be what the intruder fears most. Corrective controls, on the other hand, are not preventive or detective, but they are clearly linked with technical controls when antiviral software eradicates a virus or with administrative controls when backup procedures enable restoring a damaged data base. Finally, recovery controls are neither preventive nor detective but are included in administrative controls as disaster recovery or contingency plans.

QUESTION NO: 6

クライアントとサーバー間の通信に RADIUS で使用されるのは次のうちどれですか?

A. TCP

B. SSL
C.UDP
D. SSH
Answer: C

QUESTION NO: 7
サーバー クラスターは次のようになります。
A. ユーザーから見た単一サーバー
B. ユーザーから見たデュアルサーバー
C. ユーザーから見たトリプルサーバー
D. ユーザーの視点から見た quardle サーバー
Answer: A
Explanation:
Fiber Optic cable is immune to the effects of electromagnetic interference (EMI) and therefore has a much longer effective usable length (up to two kilometers in some cases).

QUESTION NO: 8
Bell-LaPadula モデルでは、Star プロパティは次のようにも呼ばれます。
A. シンプルなセキュリティ プロパティ
B. 機密性プロパティ
C. 閉じ込め特性
D. 静けさの性質
Answer: B
Explanation:
The Bell-LaPadula model focuses on data confidentiality and access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity.
In this formal model, the entities in an information system are divided into subjects and objects.
The notion of a "secure state" is defined, and it is proven that each state transition preserves security by moving from secure state to secure state, thereby proving that the system satisfies the security objectives of the model.
The Bell-LaPadula model is built on the concept of a state machine with a set of allowable states in a system. The transition from one state to another state is defined by transition functions.
A system state is defined to be "secure" if the only permitted access modes of subjects to objects are in accordance with a security policy.
To determine whether a specific access mode is allowed, the clearance of a subject is compared to the classification of the object (more precisely, to the combination of classification and set of compartments, making up the security level) to determine if the subject is authorized for the specific access mode.
The clearance/classification scheme is expressed in terms of a lattice. The model defines two mandatory access control (MAC) rules and one discretionary access control (DAC) rule with three security properties:

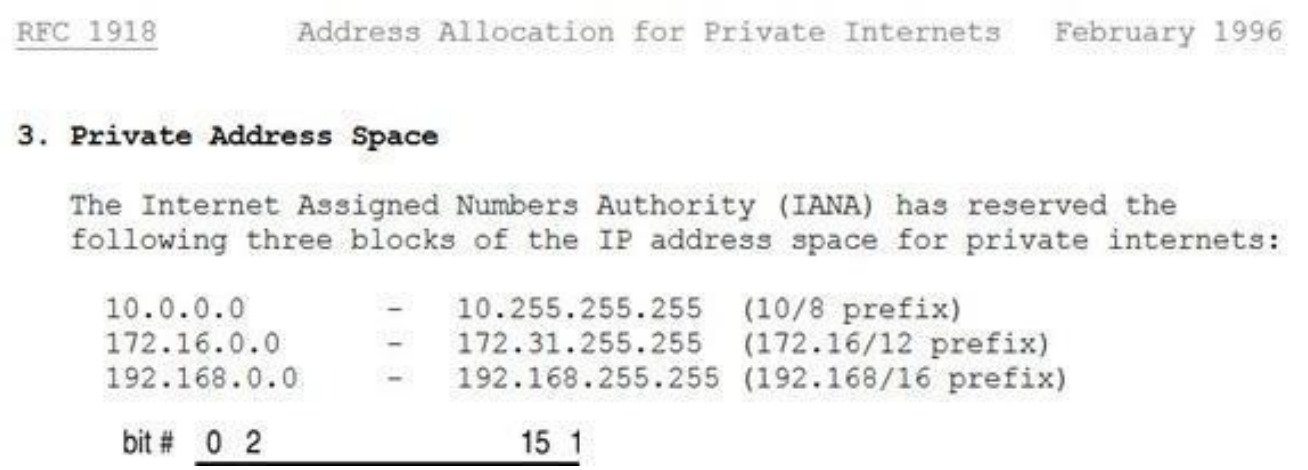
The Simple Security Property - a subject at a given security level may not read an object at a higher security level (no read-up).
The property (read "star"-property) - a subject at a given security level must not write to any object at a lower security level (no write-down). The property is also known as the Confinement property.
The Discretionary Security Property - use an access control matrix to specify the discretionary access control.
The transfer of information from a high-sensitivity document to a lower-sensitivity document may happen in the Bell-LaPadula model via the concept of trusted subjects. Trusted Subjects are not restricted by the property. Untrusted subjects are.
Trusted Subjects must be shown to be trustworthy with regard to the security policy. This security model is directed toward access control and is characterized by the phrase: "no read up, no write down." Compare the Biba model, the Clark-Wilson model and the Chinese Wall.
With Bell-LaPadula, users can create content only at or above their own security level (i.e. secret researchers can create secret or top-secret files but may not create public files; no write-down).
Conversely, users can view content only at or below their own security level (i.e. secret researchers can view public or secret files, but may not view top-secret files; no read-up).
Strong Property
The Strong Property is an alternative to the Property in which subjects may write to objects with only a matching security level. Thus, the write-up operation permitted in the usual Property is not present, only a write-to-same level operation. The Strong Property is usually discussed in the context of multilevel database management systems and is motivated by integrity concerns.
Tranquility principle
The tranquility principle of the Bell-LaPadula model states that the classification of a subject or object does not change while it is being referenced. There are two forms to the tranquility principle:
the "principle of strong tranquility" states that security levels do not change during the normal operation of the system and the "principle of weak tranquility" states that security levels do not change in a way that violates the rules of a given security policy.
Another interpretation of the tranquility principles is that they both apply only to the period of time during which an operation involving an object or subject is occurring. That is, the strong tranquility principle means that an object's security level/label will not change during an operation (such as read or write); the weak tranquility principle means that an object's security level/label may change in a way that does not violate the security policy during an operation.

QUESTION NO: 9
次のうち、リスク評価システムではないものはどれですか?
A. 総合対策効果 (ACE) モデル
B. 情報セキュリティ保護評価モデル (ISPAM)
C. ドルベースの OPSEC リスク分析 (DORA)
D. ネットワーク化されたシステムのセキュリティ リスクの分析 (ANSSR)
Answer: B

QUESTION NO: 10
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 テストでは、ボトムアップ アプローチが使用されます。
C. ホワイトボックス テストでは、プログラムの内部論理構造を調べます。
D. ビジネス ユニットが関与するブラック ボックス テスト
Answer: C
Explanation:
Black-box testing observes the system external behavior, while white-box testing is a detailed exam of a logical path, checking the possible conditions.

QUESTION NO: 11
同じシリアル リンクで複数のネットワーク
タイプをサポートするように設計されているのは、次のうちどれですか?
A. イーサネット
B.スリップ
C.PPP
D.PPTP
Answer: B
Explanation:
A routing table is used when a destination IP address is not located on the current LAN segment.
It consists of a list of station and network addresses and a corresponding gateway IP address further along to which a routing equipment should send packets that match that station or network address. A list of IP addresses and corresponding MAC addresses is an ARP table. A DNS is used to match host names and corresponding IP addresses. The last choice is a distracter.

QUESTION NO: 12
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. syn スキャン。
B. ハーフ ポート スキャン。
C. バッファ オーバーフロー攻撃。
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: A
Explanation:
This is a valid Class C reserved address. For Class C, the reserved addresses are 192.168.0.0 - 192.168.255.255.
The private IP address ranges are defined within RFC 1918:
RFC 1918 private ip address range


RFC 1918 Address Allocation for Private Internets February 1996

3. Private Address Space

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets:

10.0.0.0	-	10.255.255.255	(10/8 prefix)
172.16.0.0	-	172.31.255.255	(172.16/12 prefix)
192.168.0.0	-	192.168.255.255	(192.168/16 prefix)

bit # 0 2 15 1

The following answers are incorrect:
192.166.42.5 Is incorrect because it is not a Class C reserved address.
192.175.42.5 Is incorrect because it is not a Class C reserved address.
192.1.42.5 Is incorrect because it is not a Class C reserved address.

QUESTION NO: 13
DES はどのアルゴリズムから派生しましたか?
A. 二匹の魚。
B. カツオ。
C. ブルックス-オールデマン。
D. ルシファー。
Answer: A
Explanation:
A Public Key is also known as an asymmetric algorithm and the use of a secret key would be a symmetric algorithm.
The following answers are incorrect:
Use of the recipient's public key for encryption and decryption based on the recipient's private key. Is incorrect this would be known as an asymmetric algorithm. Use of software encryption assisted by a hardware encryption accelerator. This is incorrect, it is a distractor.
Use of Elliptic Curve Encryption. Is incorrect this would use an asymmetric algorithm.

QUESTION NO: 14
伝聞証拠に対する業務免除規則の下で、次の例外のうち、法廷で監査ログと監査証跡が認められないことに関係のないものはどれですか?
A. 通常の業務において記録を収集します。
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.
調査対象の行為の発生時またはその近くで記録が収集され、自動レポートが生成されます。
D. 収集された記録/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: C
Explanation:
RFC 2828 (Internet Security Glossary) defines a Computer Security Incident Response Team (CSIRT) as an organization that coordinates and supports the response to security incidents

that involves sites within a defined constituency. This is the proper definition for the CSIRT. To be considered a CSIRT, an organization must provide a secure channel for receiving reports about suspected security incidents, provide assistance to members of its constituency in handling the incidents and disseminate incident-related information to its constituency and other involved parties. Security-related incidents do not necessarily have to be reported to the authorities.

QUESTION NO: 15
適切な職務分掌の主な目的は何ですか?
A. 従業員が機密情報を開示するのを防ぐため。
B. アクセス制御が実施されていることを確認するため。
C. 1 人の個人がシステムを侵害できないようにするため。
D. 監査証跡が改ざんされないようにするため。
Answer: C
Explanation:
The primary objective of proper separation of duties is to ensure that one person acting alone cannot compromise the company's security in any way. A proper separation of duties does not prevent employees from disclosing information, nor does it ensure that access controls are in place or that audit trails are not tampered with.

QUESTION NO: 16
ISO/OSI モデルのレイヤ 4 からレイヤ 7 までの 2
つのネットワークまたはアプリケーションを接続するために、トランスレータとして機能するデバイスはどれですか?
A. ブリッジ
B. リピーター
C. ルーター
D. ゲートウェイ
Answer: B
Explanation:
A modem is a device that translates data from digital form and then back to digital for communication over analog lines.

QUESTION NO: 17
データを暗号化または復号化する場合、次のようなプロセスで比較される 1 と 0
を含む基本的な操作があります。
0101 0001 平文
0111 0011 キーストリーム
0010 0010 出力
この暗号操作は何と呼ばれますか?
A. 排他的論理和
B. ビットスワップ
C. 論理 NOR
D. 復号化

Answer: A
Explanation:
The basic power in cryptography is randomness. This uncertainty is why encrypted data is unusable to someone without the key to decrypt.
Initialization Vectors are a used with encryption keys to add an extra layer of randomness to encrypted data. If no IV is used the attacker can possibly break the keyspace because of patterns resulting in the encryption process. Implementation such as DES in Code Book Mode (CBC) would allow frequency analysis attack to take place.
In cryptography, an initialization vector (IV) or starting variable (SV)is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom.
Randomization is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message. For block ciphers, the use of an IV is described by so-called modes of operation. Randomization is also required for other primitives, such as universal hash functions and message authentication codes based thereon.
It is define by TechTarget as:
An initialization vector (IV) is an arbitrary number that can be used along with a secret key for data encryption. This number, also called a nonce, is employed only one time in any session. The use of an IV prevents repetition in data encryption, making it more difficult for a hacker using a dictionary attack to find patterns and break a cipher. For example, a sequence might appear twice or more within the body of a message. If there are repeated sequences in encrypted data, an attacker could assume that the corresponding sequences in the message were also identical.
The IV prevents the appearance of corresponding duplicate character sequences in the ciphertext.
The following answers are incorrect:
- Stream Cipher: This isn't correct. A stream cipher is a symmetric key cipher where plaintext digits are combined with pseudorandom key stream to product cipher text.
- OTP - One Time Pad: This isn't correct but OTP is made up of random values used as ke y material. (Encryption key) It is considered by most to be unbreakable but must be changed with a new key after it is used which makes it impractical for common use.
- Ciphertext: Sorry, incorrect answer. Ciphertext is basically text that has been encrypted with key material (Encryption key)

QUESTION NO: 18
仮想プライベート
ネットワークを作成する際に、現在使用されていない可能性が高いのは次のうちどれですか？
A. L2TP
B.PPTP
C. IPSec
D. L2F
Answer: B
Explanation:

The SHA-1 is a hashing algorithm producing a 160-bit hash result from any data. It does not perform encryption.
In cryptography, SHA-1 is a cryptographic hash function designed by the United States National Security Agency and published by the United States NIST as a U.S. Federal Information Processing Standard.
SHA stands for "secure hash algorithm". The four SHA algorithms are structured differently and are distinguished as SHA-0, SHA-1, SHA-2, and SHA-3. SHA-1 is very similar to SHA-0, but corrects an error in the original SHA hash specification that led to significant weaknesses. The SHA-0 algorithm was not adopted by many applications. SHA-2 on the other hand significantly differs from the SHA-1 hash function.
SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols.
In 2005, cryptanalysts found attacks on SHA-1 suggesting that the algorithm might not be secure enough for ongoing use. NIST required many applications in federal agencies to move to SHA-2 after 2010 because of the weakness. Although no successful attacks have yet been reported on SHA-2, they are algorithmically similar to SHA-1.
In 2012, following a long-running competition, NIST selected an additional algorithm, Keccak, for standardization as SHA-3 NOTE:
A Cryptographic Hash Function is not the same as an Encryption Algorithm even thou both are Algorithms. An algorithm is defined as a step-by-step procedure for calculations. Hashing Algorithm do not encrypt the data. People sometimes will say they encrypted a password with SHA-1 but really they simply created a Message Digest of the password using SHA-1, putting the input through a series of steps to come out with the message digest or hash value.
A cryptographic hash function is a hash function; that is, an algorithm that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that any (accidental or intentional) change to the data will (with very high probability) change the hash value. The data to be encoded are often called the "message," and the hash value is sometimes called the message digest or simply digest.
Encryption Algorithms are reversible but Hashing Algorithms are not meant to be reversible if the input is large enough.
The following are incorrect answers:
The Skipjack algorithm is a Type II block cipher with a block size of 64 bits and a key size of 80 bits that was developed by NSA and formerly classified at the U.S. Department of Defense
"Secret" level.
Twofish is a freely available 128-bit block cipher designed by Counterpane Systems (Bruce Schneier et al.).
DEA is a symmetric block cipher, defined as part of the U.S. Government's Data Encryption Standard (DES). DEA uses a 64-bit key, of which 56 bits are independently chosen and 8 are parity bits, and maps a 64-bit block into another 64-bit block.

QUESTION NO: 19
システムアカウンタビリティに必要なものは次のうちどれですか?
A. 監査メカニズム。
B. Common Criteria に記載されている文書化された設計。

C. 承認。
D. システム設計の正式な検証。
Answer: A
Explanation:
Is a means of being able to track user actions. Through the use of audit logs and other tools the user actions are recorded and can be used at a later date to verify what actions were performed.
Accountability is the ability to identify users and to be able to track user actions.
The following answers are incorrect:
Documented design as laid out in the Common Criteria. Is incorrect because the Common Criteria is an international standard to evaluate trust and would not be a factor in System Accountability.
Authorization. Is incorrect because Authorization is granting access to subjects, just because you have authorization does not hold the subject accountable for their actions.
Formal verification of system design. Is incorrect because all you have done is to verify the system design and have not taken any steps toward system accountability.

QUESTION NO: 20
デジタル署名が実行する最も重要な機能を 3 つ挙げてください。
A. 整合性、機密性、および承認
B. 整合性、認証、否認防止
C. 承認、認証、否認防止
D. 承認、検出、説明責任
Answer: A
Explanation:
SET was developed by a consortium including Visa and MasterCard.
Mondex is a smart card electronic cash system owned by MasterCard. SSH-2 is a secure, efficient, and portable version of SSH (Secure Shell) which is a secure replacement for telnet .
Secure HTTP is a secure message-oriented communications protocol designed for use in conjunction with HTTP. It is designed to coexist with HTTP's messaging model and to be easily integrated with HTTP applications.

QUESTION NO: 21
次のコンピュータ設計アプローチのうち、以前のテクノロジでは命令フェッチがサイクルの最も長い部分であったという事実に基づいているのはどれですか?
A. パイプライン
B. 縮小命令セット コンピューター (RISC)
C. 複合命令セット コンピュータ (CISC)
D. スカラー プロセッサ
Answer: C
Explanation:
A fault-tolerant system is capable of detecting that a fault has occurred and has the ability to correct the fault or operate around it. In a fail-safe system, program execution is terminated,

and the system is protected from being compromised when a hardware or software failure occurs and is detected. In a fail-soft system, when a hardware or software failure occurs and is detected, selected, non-critical processing is terminated. The term failover refers to switching to a duplicate
"hot" backup component in real-time when a hardware or software failure occurs, enabling processing to continue.

QUESTION NO: 22
次のうち、Kerberos について正しいものはどれですか?
A. 公開鍵暗号方式を利用しています。
B. チケットが付与された後にデータを暗号化しますが、パスワードは平文で交換されます。
C. 対称暗号に依存します。
D. 第二者認証方式です。
Answer: C
Explanation:
Kerberos depends on secret keys (symmetric ciphers). Kerberos is a third party authentication protocol. It was designed and developed in the mid 1980's by MIT. It is considered open source but is copyrighted and owned by MIT. It relies on the user's secret keys. The password is used to encrypt and decrypt the keys.
The following answers are incorrect:
It utilizes public key cryptography. Is incorrect because Kerberos depends on secret keys (symmetric ciphers).
It encrypts data after a ticket is granted, but passwords are exchanged in plain text. Is incorrect because the passwords are not exchanged but used for encryption and decryption of the keys.
It is a second party authentication system. Is incorrect because Kerberos is a third party authentication system, you authenticate to the third party (Kerberos) and not the system you are accessing.

QUESTION NO: 23
プログラムのデバッグの目的を最もよく表しているのは次のうちどれですか?
A. プログラムを実装する前にテストするために使用できるランダム
データを生成すること。
B. プログラムのコーディング上の欠陥を確実に検出して修正するため。
C. プログラミング
フェーズ中に、有効な変更が他の変更によって上書きされないように保護します。
D. テスト環境に移行する前にソース コードのバージョンを比較するには
Answer: B
Explanation:
Debugging provides the basis for the programmer to correct the logic errors in a program under development before it goes into production.

QUESTION NO: 24
MD5 は _____ アルゴリズムです
A. 一方向ハッシュ

B. 3DES
C. 192 ビット
D. PKI
Answer: A

QUESTION NO: 25
非任意アクセス制御 (NDAC) とも呼ばれるアクセス制御モデルは?
A. 格子ベースのアクセス制御
B. 強制アクセス制御
C. ロールベースのアクセス制御
D. ラベルベースのアクセス制御
Answer: C
Explanation:
RBAC is sometimes also called non-discretionary access control (NDAC) (as Ferraiolo says "to distinguish it from the policy-based specifics of MAC"). Another model that fits within the NDAC category is Rule-Based Access Control (RuBAC or RBAC). Most of the CISSP books use the same acronym for both models but NIST tend to use a lowercase "u" in between R and B to differentiate the two models.
You can certainly mimic MAC using RBAC but true MAC makes use of Labels which contains the sensitivity of the objects and the categories they belong to. No labels means MAC is not being used.
One of the most fundamental data access control decisions an organization must make is the amount of control it will give system and data owners to specify the level of access users of that data will have. In every organization there is a balancing point between the access controls enforced by organization and system policy and the ability for information owners to determine who can have access based on specific business requirements. The process of translating that balance into a workable access control model can be defined by three general access frameworks:
Discretionary access control
Mandatory access control
Nondiscretionary access control
A role-based access control (RBAC) model bases the access control authorizations on the roles (or functions) that the user is assigned within an organization. The determination of what roles have access to a resource can be governed by the owner of the data, as with DACs, or applied based on policy, as with MACs.
Access control decisions are based on job function, previously defined and governed by policy, and each role (job function) will have its own access capabilities. Objects associated with a role will inherit privileges assigned to that role. This is also true for groups of users, allowing administrators to simplify access control strategies by assigning users to groups and groups to roles.
There are several approaches to RBAC. As with many system controls, there are variations on how they can be applied within a computer system.
There are four basic RBAC architectures:
1. Non-RBAC: Non-RBAC is simply a user-granted access to data or an application by traditional mapping, such as with ACLs. There are no formal "roles" associated with the

mappings, other than any identified by the particular user.
2. Limited RBAC: Limited RBAC is achieved when users are mapped to roles within a single application rather than through an organization-wide role structure. Users in a limited RBAC system are also able to access non-RBAC-based applications or data. For example, a user may be assigned to multiple roles within several applications and, in addition, have direct access to another application or system independent of his or her assigned role. The key attribute of limited RBAC is that the role for that user is defined within an application and not necessarily based on the user's organizational job function.
3. Hybrid RBAC: Hybrid RBAC introduces the use of a role that is applied to multiple applications or systems based on a user's specific role within the organization. That role is then applied to applications or systems that subscribe to the organization's role-based model. However, as the term "hybrid" suggests, there are instances where the subject may also be assigned to roles defined solely within specific applications, complimenting (or, perhaps, contradicting) the larger, more encompassing organizational role used by other systems.
4. Full RBAC: Full RBAC systems are controlled by roles defined by the organization's policy and access control infrastructure and then applied to applications and systems across the enterprise.
The applications, systems, and associated data apply permissions based on that enterprise definition, and not one defined by a specific application or system. Be careful not to try to make MAC and DAC opposites of each other -- they are two different access control strategies with RBAC being a third strategy that was defined later to address some of the limitations of MAC and DAC.
The other answers are not correct because:
Mandatory access control is incorrect because though it is by definition not discretionary, it is not called "non-discretionary access control." MAC makes use of label to indicate the sensitivity of the object and it also makes use of categories to implement the need to know.
Label-based access control is incorrect because this is not a name for a type of access control but simply a bogus detractor.
Lattice based access control is not adequate either. A lattice is a series of levels and a subject will be granted an upper and lower bound within the series of levels. These levels could be sensitivity levels or they could be confidentiality levels or they could be integrity levels.

QUESTION NO: 26
次のうち、静的パスワード トークンについて正しいものはどれですか?
A. 所有者 ID はトークンによって認証されます
B. トークンによって所有者が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
Explanation:
Password Tokens
Tokens are electronic devices or cards that supply a user's password for them. A token system can be used to supply either a static or a dynamic password. There is a big difference between the static and dynamic systems, a static system will normally log a user in but a

dynamic system the user will often have to log themselves in.
Static Password Tokens:
The owner identity is authenticated by the token. This is done by the person who issues the token to the owner (normally the employer). The owner of the token is now authenticated by "something you have". The token authenticates the identity of the owner to the information system. An example of this occurring is when an employee swipes his or her smart card over an electronic lock to gain access to a store room.
Synchronous Dynamic Password Tokens:
This system is a lot more complex then the static token password. The synchronous dynamic password tokens generate new passwords at certain time intervals that are synched with the main system. The password is generated on a small device similar to a pager or a calculator that can often be attached to the user's key ring. Each password is only valid for a certain time period, typing in the wrong password in the wrong time period will invalidate the authentication. The time factor can also be the systems downfall. If a clock on the system or the password token device becomes out of synch, a user can have troubles authenticating themselves to the system.
Asynchronous Dynamic Password Tokens:
The clock synching problem is eliminated with asynchronous dynamic password tokens. This system works on the same principal as the synchronous one but it does not have a time frame. A lot of big companies use this system especially for employee's who may work from home on the companies VPN (Virtual private Network).
Challenge Response Tokens:
This is an interesting system. A user will be sent special "challenge" strings at either random or timed intervals. The user inputs this challenge string into their token device and the device will respond by generating a challenge response. The user then types this response into the system and if it is correct they are authenticated.

QUESTION NO: 27
パスワード管理は、どの制御カテゴリに分類されますか?
A.補正中
B. 探偵
C. 予防
D. テクニカル
Answer: C
Explanation:
Password management is an example of preventive control. Proper passwords prevent unauthorized users from accessing a system.
There are literally hundreds of different access approaches, control methods, and technologies, both in the physical world and in the virtual electronic world. Each method addresses a different type of access control or a specific access need.
For example, access control solutions may incorporate identification and authentication mechanisms, filters, rules, rights, logging and monitoring, policy, and a plethora of other controls.
However, despite the diversity of access control methods, all access control systems can be categorized into seven primary categories.

The seven main categories of access control are:
1. Directive: Controls designed to specify acceptable rules of behavior within an organization
2. Deterrent: Controls designed to discourage people from violating security directives
3. Preventive: Controls implemented to prevent a security incident or information breach
4. Compensating: Controls implemented to substitute for the loss of primary controls and mitigate risk down to an acceptable level
5. Detective: Controls designed to signal a warning when a security control has been breached
6. Corrective: Controls implemented to remedy circumstance, mitigate damage, or restore controls
7. Recovery: Controls implemented to restore conditions to normal after a security incident

QUESTION NO: 28
物理的なセキュリティは、適切な施設の建設、防火および防水、盗難防止メカニズム、侵入検知システム、および順守および実施されるセキュリティ手順によって達成されます。このタイプのセキュリティを実現するコンポーネントではないのは、次のうちどれですか?
A. 管理制御メカニズム
B. 完全性制御メカニズム
C. 技術的な制御メカニズム
D. 物理的な制御メカニズム
Answer: B
Explanation:
Integrity Controls Mechanisms are not part of physical security. All of the other detractors were correct this one was the wrong one that does not belong to Physical Security. Below you have more details extracted from the SearchSecurity web site:
Information security depends on the security and management of the physical space in which computer systems operate. Domain 9 of the CISSP exam's Common Body of Knowledge addresses the challenges of securing the physical space, its systems and the people who work within it by use of administrative, technical and physical controls. The following QUESTION are covered:
Facilities management: The administrative processes that govern the maintenance and protection of the physical operations space, from site selection through emergency response.
Risks, issues and protection strategies: Risk identification and the selection of security protection components.
Perimeter security: Typical physical protection controls.
Facilities management
Facilities management is a complex component of corporate security that ranges from the planning of a secure physical site to the management of the physical information system environment. Facilities management responsibilities include site selection and physical security planning (i.e. facility construction, design and layout, fire and water damage protection, antitheft mechanisms, intrusion detection and security procedures.) Protections must extend to both people and assets. The necessary level of protection depends on the value of the assets and data. CISSP?candidates must learn the concept of critical-path analysis as a means of determining a component's business function criticality relative to the cost of operation and replacement. Furthermore, students need to gain an understanding of

the optimal location and physical attributes of a secure facility. Among the QUESTION covered in this domain are site inspection, location, accessibility and obscurity, considering the area crime rate, and the likelihood of natural hazards such as floods or earthquakes. This domain also covers the quality of construction material, such as its protective qualities and load capabilities, as well as how to lay out the structure to minimize risk of forcible entry and accidental damage. Regulatory compliance is also touched on, as is preferred proximity to civil protection services, such as fire and police stations. Attention is given to computer and equipment rooms, including their location, configuration (entrance/egress requirements) and their proximity to wiring distribution centers at the site.
Physical risks, issues and protection strategies
An overview of physical security risks includes risk of theft, service interruption, physical damage, compromised system integrity and unauthorized disclosure of information. Interruptions to business can manifest due to loss of power, services, telecommunications connectivity and water supply. These can also seriously compromise electronic security monitoring alarm/response devices. Backup options are also covered in this domain, as is a strategy for quantifying the risk exposure by simple formula.
Investment in preventive security can be costly. Appropriate redundancy of people skills, systems and infrastructure must be based on the criticality of the data and assets to be preserved.
Therefore a strategy is presented that helps determine the selection of cost appropriate controls.
Among the QUESTION covered in this domain are regulatory and legal requirements, common standard security protections such as locks and fences, and the importance of establishing service level agreements for maintenance and disaster support. Rounding out the optimization approach are simple calculations for determining mean time between failure and mean time to repair (used to estimate average equipment life expectancy) -- essential for estimating the cost/benefit of purchasing and maintaining redundant equipment.
As the lifeblood of computer systems, special attention is placed on adequacy, quality and protection of power supplies. CISSP candidates need to understand power supply concepts and terminology, including those for quality (i.e. transient noise vs. clean power); types of interference (EMI and RFI); and types of interruptions such as power excess by spikes and surges, power loss by fault or blackout, and power degradation from sags and brownouts. A simple formula is presented for determining the total cost per hour for backup power. Proving power reliability through testing is recommended and the advantages of three power protection approaches are discussed (standby UPS, power line conditioners and backup sources) including minimum requirements for primary and alternate power provided.
Environmental controls are explored in this domain, including the value of positive pressure water drains and climate monitoring devices used to control temperature, humidity and reduce static electricity. Optimal temperatures and humidity settings are provided. Recommendations include strict procedures during emergencies, preventing typical risks (such as blocked fans), and the use of antistatic armbands and hygrometers. Positive pressurization for proper ventilation and monitoring for air born contaminants is stressed.
The pros and cons of several detection response systems are deeply explored in this domain.
The concept of combustion, the classes of fire and fire extinguisher ratings are detailed.

Mechanisms behind smoke-activated, heat-activated and flame-activated devices and Automatic Dial-up alarms are covered, along with their advantages, costs and shortcomings. Types of fire sources are distinguished and the effectiveness of fire suppression methods for each is included.
For instance, Halon and its approved replacements are covered, as are the advantages and the inherent risks to equipment of the use of water sprinklers.
Administrative controls
The physical security domain also deals with administrative controls applied to physical sites and assets. The need for skilled personnel, knowledge sharing between them, separation of duties, and appropriate oversight in the care and maintenance of equipment and environments is stressed. A list of management duties including hiring checks, employee maintenance activities and recommended termination procedures is offered. Emergency measures include accountability for evacuation and system shutdown procedures, integration with disaster and business continuity plans, assuring documented procedures are easily available during different types of emergencies, the scheduling of periodic equipment testing, administrative reviews of documentation, procedures and recovery plans, responsibilities delegation, and personnel training and drills.
Perimeter security
Domain nine also covers the devices and techniques used to control access to a space. These include access control devices, surveillance monitoring, intrusion detection and corrective actions. Specifications are provided for optimal external boundary protection, including fence heights and placement, and lighting placement and types. Selection of door types and lock characteristics are covered. Surveillance methods and intrusion-detection methods are explained, including the use of video monitoring, guards, dogs, proximity detection systems, photoelectric/photometric systems, wave pattern devices, passive infrared systems, and sound and motion detectors, and current flow sensitivity devices that specifically address computer theft.
Room lock types -- both preset and cipher locks (and their variations) -- device locks, such a s portable laptop locks, lockable server bays, switch control locks and slot locks, port controls, peripheral switch controls and cable trap locks are also covered. Personal access control methods used to identify authorized users for site entry are covered at length, noting social engineering risks such as piggybacking. Wireless proximity devices, both user access and system sensing readers are covered (i.e. transponder based, passive devices and field powered devices) in this domain.

QUESTION NO: 29
10Base5 とも呼ばれます。
A. シンネット
B. シックネット
C. アークネット
D. UTP
Answer: A
Explanation:
X.400 is used in e-mail as a message handling protocol. X.500 is used in directory services. X.509 is used in digital certificates and X.800 is used a network security standard.

QUESTION NO: 30
クリッピング レベルが使用されるのはなぜですか?
A. 評価するデータ量を削減します。
B. パスワード内の英数字の数を制限します
C. RADIUS システムのエラーを制限します
D. ファイルとオブジェクトのアクセスに対するしきい値のみを設定します。
Answer: A

QUESTION NO: 31
次のうち、災害復旧の観点から最も重要な項目はどれですか?
A. データ
B. ハードウェア/ソフトウェア
C. 通信リンク
D. ソフトウェア アプリケーション
Answer: D
Explanation:
All businesses are driven by records. Even in today's electronic society businesses generate mountains of critical documents everyday. Invoices, client lists, calendars, contracts, files, medical records, and innumerable other records are generated every day.
Stop and ask yourself what happens if your business lost those documents today.
Valuable papers business insurance coverage provides coverage to your business in case of a loss of vital records. Over the years policy language has evolved to include a number of different types of records. Generally, the policy will cover "written, printed, or otherwise inscribed documents and records, including books, maps, films, drawings, abstracts, deeds, mortgages, and manuscripts." But, read the policy coverage carefully. The policy language typically "does not mean "money" or "securities," converted data,programs or instructions used in your data processing operations, including the materials on which the data is recorded." The coverage is often included as a part of property insurance or as part of a small business owner policy. For example, a small business owner policy includes in many cases valuable papers coverage up to $25,000.
It is important to realize what the coverage actually entails and, even more critical, to analyze your business to determine what it would cost to replace records.
The coverage pays for the loss of vital papers and the cost to replace the records up to the limit of the insurance and after application of any deductible. For example, the insurer will pay to have waterlogged papers dried and reproduced (remember, fires are put out by water and the fire department does not stop to remove your book keeping records). The insurer may cover temporary storage or the cost of moving records to avoid a loss.
For some businesses, losing customer lists, some business records, and contracts, can mean the expense and trouble of having to recreate those documents, but is relatively easy and a low level risk and loss. Larger businesses and especially professionals (lawyers, accountants, doctors) are in an entirely separate category and the cost of replacement of documents is much higher.
Consider, in analyzing your business and potential risk, what it would actually cost to reproduce your critical business records. Would you need to hire temporary personnel? How

many hours of productivity would go into replacing the records? Would you need to obtain originals? Would original work need to be recreated (for example, home inspectors, surveyors, cartographers)?
Often when a business owner considers the actual cost related to the reproduction of records, the owner quickly realizes that their business insurance policy limits for valuable papers coverage is woefully inadequate.
Insurers (and your insurance professional)will often suggest higher coverages for valuable papers. The extra premium is often worth the cost and should be considered.
Finally, most policies will require records to be protected. You need to review your declarations pages and speak with your insurer to determine what is required. Some insurers may offer discounted coverage if there is a document retention and back up plan in place and followed.
There are professional organizations that can assist your business in designing a records management policy to lower the risk (and your premiums). For example, ARMA International has been around since 1955 and its members consist of some of the top document retention and storage companies.

QUESTION NO: 32
プロキシは、受け入れられた各データ
パケットのコピーをある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、それによって次のものをマスキングします。
A. データのペイロード
B. データの詳細
C. データの所有者
D. データの起源
Answer: C
Explanation:
The proxy (application layer firewall, circuit level proxy, or application proxy) is a second generation firewall
"First generation firewall" incorrect. A packet filtering firewall is a first generation firewall.
"Third generation firewall" is incorrect. Stateful Firewall are considered third generation firewalls "Fourth generation firewall" is incorrect. Dynamic packet filtering firewalls are fourth generation firewalls

QUESTION NO: 33
_____ は、TCP 3 ウェイ
ハンドシェイクを中断し、接続を半分開いたままにするサービス拒否攻撃の一種です。
A. DNS 再帰
B. NMAP
C. 陸上攻撃
D. SYN フラッディング
E. ポートスキャン
Answer: D

QUESTION NO: 34

CAT3 および CAT5 カテゴリに該当するケーブル技術はどれですか?
A. 同軸ケーブル
B. 光ファイバーケーブル
C. 軸ケーブル
D. ツイストペアケーブル
Answer: A
Explanation:
FDDI is a token-passing ring scheme like a token ring, yet it also has a second ring that remains dormant until an error condition is detected on the primary ring.
Fiber Distributed Data Interface (FDDI) provides a 100 Mbit/s optical standard for data transmission in a local area network that can extend in range up to 200 kilometers (124 miles).
Although FDDI logical topology is a ring-based token network, it does not use the IEEE 802.5 token ring protocol as its basis; instead, its protocol is derived from the IEEE 802.4 token bus timed token protocol. In addition to covering large geographical areas, FDDI local area networks can support thousands of users. As a standard underlying medium it uses optical fiber, although it can use copper cable, in which case it may be refer to as CDDI (Copper Distributed Data Interface). FDDI offers both a Dual-Attached Station (DAS), counter-rotating token ring topology and a Single-Attached Station (SAS), token bus passing ring topology.
Ethernet is a family of frame-based computer networking technologies for local area networks (LANs). The name came from the physical concept of the ether. It defines a number of wiring and signaling standards for the Physical Layer of the OSI networking model as well as a common addressing format and Media Access Control at the Data Link Layer.
In computer networking, Fast Ethernet is a collective term for a number of Ethernet standards that carry traffic at the nominal rate of 100 Mbit/s, against the original Ethernet speed of 10 Mbit/s. Of the fast Ethernet standards 100BASE-TX is by far the most common and is supported by the vast majority of Ethernet hardware currently produced. Fast Ethernet was introduced in 1995 and remained the fastest version of Ethernet for three years before being superseded by gigabit Ethernet.
Broadband in data can refer to broadband networks or broadband Internet and may have the same meaning as above, so that data transmission over a fiber optic cable would be referred to as broadband as compared to a telephone modem operating at 56,000 bits per second. However, a worldwide standard for what level of bandwidth and network speeds actually constitute Broadband have not been determined.[1] Broadband in data communications is frequently used in a more technical sense to refer to data transmission where multiple pieces of data are sent simultaneously to increase the effective rate of transmission, regardless of data signaling rate. In network engineering this term is used for methods where two or more signals share a medium.[Broadband Internet access, often shortened to just broadband, is a high data rate Internet access--typically contrasted with dial-up access using a 56k modem. Dial-up modems are limited to a bitrate of less than 56 kbit/s (kilobits per second) and require the full use of a telephone line--whereas broadband technologies supply more than double this rate and generally without disrupting telephone use.

QUESTION NO: 35
以下のそれぞれは、_____ を除き、インシデントを処理する際の有効な手順です。

A. を含む
B. 起訴する
C. 回復します
D. レビュー
E. 識別
F. 準備します
Answer: B