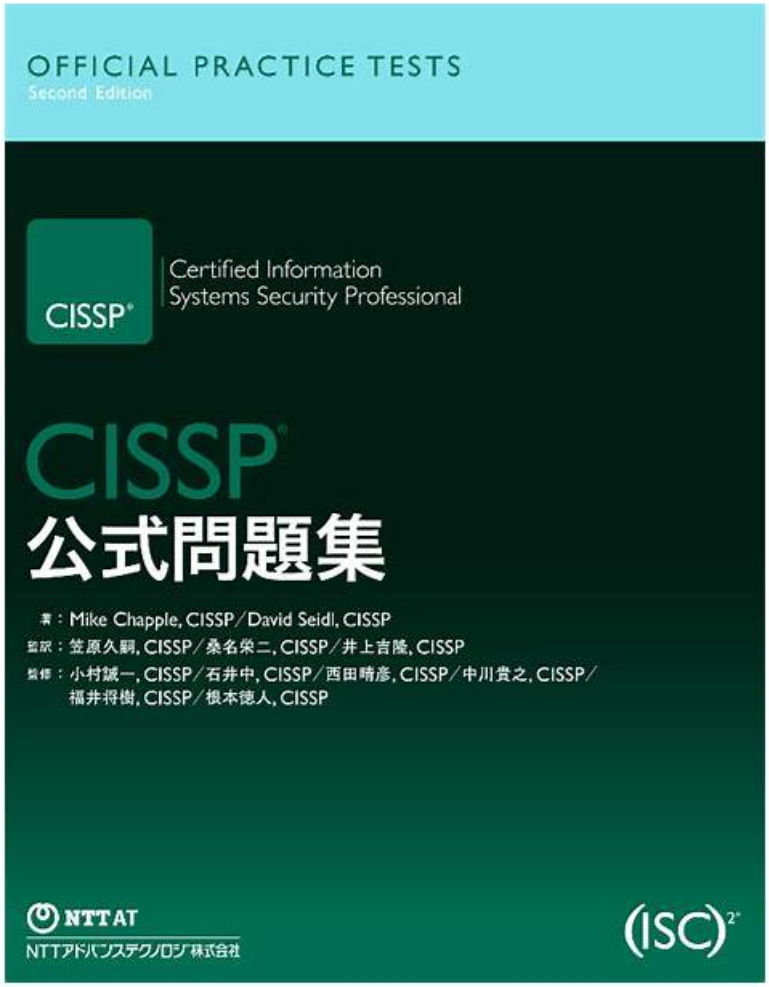
ハイパスレートのCISSP練習問題集 &合格スムーズCISSP日本語講座 |ユニークなCISSP日本語版トレーリング



2025年Tech4Examの最新CISSP PDFダンプおよびCISSP試験エンジンの無料共有：https://drive.google.com/open?id=1bUk3SNBc_qmzDTicPX6euX3-3MFiPeU4

クライアントはCISSP試験問題を学習し、テストの準備をするのに20〜30時間しかかかりません。多くの人は、CISSPテストの準備が必要だと不満を言うかもしれませんが、一方でTech4Exam、仕事、学習、家族などの最も重要なことにほとんどの時間を費やさなければなりません。ただし、CISSP学習ガイドを購入すると、テストの準備に時間と労力がほとんどかからないため、最も重要なことをうまくやり、CISSPテストに簡単に合格できます。

ISC CISSP認定を達成することは、情報セキュリティの専門家に対する高レベルの専門知識とコミットメントを示しています。キャリアの機会を強化し、可能性を獲得し、雇用市場で競争上の優位性をもたらすことができます。さらに、政府、軍事、民間組織における多くの上級レベルの情報セキュリティの役割の要件です。全体として、ISC CISSP認定試験は、自分のスキルを検証し、キャリアを促進しようとしている情報セキュリティの専門家にとって、挑戦的であるがやりがいのある仕事です。

CISSP認定試験は、情報セキュリティに関連する幅広いトピックをカバーしています。この試験は、情報セキュリティの概念、テクニック、ベストプラクティスに関する候補者の知識と理解をテストするように設計されています。試験で取り上げられているトピックには、セキュリティとリスク管理、資産セキュリティ、セキュリティエンジニアリング、コミュニケーションとネットワークセキュリティ、ソフトウェア開発セキュリティが含まれます。この試験では、セキュリティ業務とビジネスの継続性に関連するトピックもカバーしています。

CISSP日本語講座 & CISSP日本語版トレーリング

Tech4Examについてどのくらい知っているのですか。Tech4ExamのCISSP試験問題集を利用したことがありますか。あるいは、知人からTech4Examを聞いたことがありますか。IT認定試験に関連する参考書のプロな提供者として、Tech4Examは間違いなくあなたが今まで見た最高のサイトです。なぜこのように確かめるのですか。それはTech4Examのように最良のCISSP試験参考書を提供してあなたに試験に合格させるだけでなく、最高品質のサービスを提供してあなたに100%満足させることもできるサイトがないからです。

ISC Certified Information Systems Security Professional (CISSP) 認定 CISSP 試験問題 (Q939-Q944):

質問 # 939
What is the minimum static charge able to cause disk drive data loss?

- A. 1500 volts
- B. 550 volts
- C. 1000 volts
- D. 2000 volts

正解：A

解説：
A static charge of 1500 volts is able to cause disk drive data loss.
A charge of 1000 volts is likely to scramble monitor display and a charge of 2000 volts can cause a system shutdown.
It should be noted that charges of up to 20,000 volts or more are possible under conditions of very low humidity with non-static-free carpeting.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the
Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 10: Physical
Security (page 333).

質問 # 940
Behavioral-based systems are also known as?

- A. Pattern matching systems
- B. Rule-based IDS
- C. Misuse detective systems
- D. Profile-based systems

正解：D

解説：
There are two complementary approaches to detecting intrusions, knowledge-based approaches and behavior-based approaches. This entry describes the second approach. It must be noted that very few tools today implement such an approach, even if the founding Denning paper {D. Denning, An Intrusion Detection Model, IEEE transactions on software engineering} recognizes this as a requirement for IDS systems.
Behavior-based intrusion detection techniques assume that an intrusion can be detected by observing a deviation from normal or expected behavior of the system or the users. The model of normal or valid behavior is extracted from reference information collected by various means. The intrusion detection system later compares this model with the current activity. When a deviation is observed, an alarm is generated. In other words, anything that does not correspond to a previously learned behavior is considered intrusive. Therefore, the intrusion detection system might be complete (i.e. all attacks should be caught), but its accuracy is a difficult issue (i.e. you get a lot of false alarms).
Advantages of behavior-based approaches are that they can detect attempts to exploit new and unforeseen vulnerabilities. They can even contribute to the (partially) automatic discovery of these new attacks. They are less dependent on operating system-specific mechanisms. They also help detect 'abuse of privileges' types of attacks that do not actually involve exploiting any security vulnerability. In short, this is the paranoid approach: Everything which has not been seen previously is dangerous.
The high false alarm rate is generally cited as the main drawback of behavior-based techniques because the entire scope of the

behavior of an information system may not be covered during the learning phase. Also, behavior can change over time, introducing the need for periodic online retraining of the behavior profile, resulting either in unavailability of the intrusion detection system or in additional false alarms. The information system can undergo attacks at the same time the intrusion detection system is learning the behavior. As a result, the behavior profile contains intrusive behavior, which is not detected as anomalous.
Herve Debar
IBM Zurich Research Laboratory
The following answers are incorrect:
Pattern matching systems are signature-based (e.g. Anti-virus).
Misuse detection systems is another name for signature-based IDSs.
Rule-based IDS is a distractor.
The following reference(s) were/was used to create this question:
Shon Harris AIO - 4th edition, Page 254
and
http://www.sans.org/security-resources/idfaq/behavior_based.php

質問 # 941
A software developer wishes to write code that will execute safely and only as intended. Which of the following programming language types is MOST likely to achieve this goal?

- A. Weakly typed
- B. Statically typed
- C. Strongly typed
- D. Dynamically typed

正解：D

質問 # 942
Which of the following security control is intended to avoid an incident from occurring?

- A. Recovery
- B. Preventive
- C. Corrective
- D. Deterrent

正解：B

解説：
Preventive controls are intended to avoid an incident from occurring For your exam you should know below information about different security controls
Deterrent Controls Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions. The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events. When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs. It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.
Preventative Controls Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative

controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.
Compensating Controls Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk. For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement. Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.
Detective Controls Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk. As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system. This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.
Corrective Controls When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.
Recovery Controls Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management. Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install. Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.
The following answers are incorrect:
Deterrent - Deterrent controls are intended to discourage a potential attacker
Corrective - Corrective control fixes components or systems after an incident has occurred
Recovery - Recovery controls are intended to bring the environment back to regular operations
The following reference(s) were/was used to create this question:
CISA Review Manual 2014 Page number 44 and Official ISC2 CISSP guide 3rd edition Page number 50 and 51

質問 # 943
When backing up an applications system's data, which of the following is a key question to be answered first?

- A. How to store backups
- B. Where to keep backups
- C. When to make backups
- D. What records to backup

正解：D

解説：
It is critical that a determination be made of WHAT data is important and should be
retained and protected. Without determining the data to be backed up, the potential for error
increases. A record or file could be vital and yet not included in a backup routine. Alternatively,

temporary or insignificant files could be included in a backup routine unnecessarily.
The following answers were incorrect:
When to make backups Although it is important to consider schedules for backups, this is done after the decisions are made of what should be included in the backup routine.
Where to keep backups The location of storing backup copies of data (Such as tapes, on-line backups, etc) should be made after determining what should be included in the backup routine and the method to store the backup.
How to store backups The backup methodology should be considered after determining what data should be included in the backup routine.

質問 # 944
......