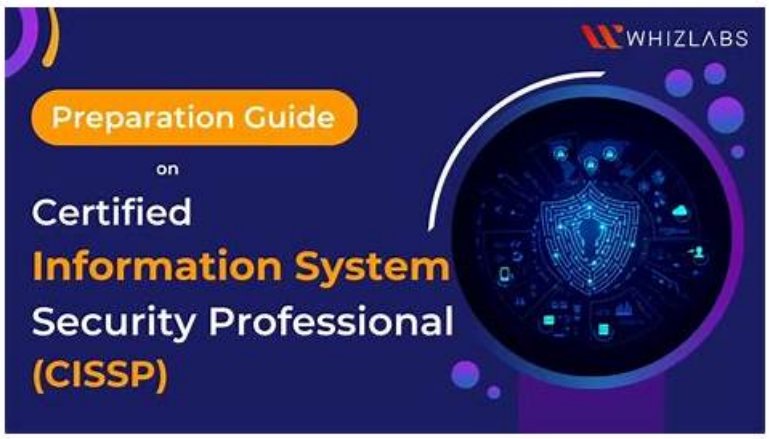
# CISSP日本語独学書籍 - Certified Information Systems Security Professional (CISSP)に合格するための親友




P.S.JpshikenがGoogle Driveで共有している無料の2025 ISC CISSPダンプ：https://drive.google.com/open?id=1v_xf_JOXJm31VCaJQbLzcM43tPXsJQNN

最近、ISC問題集を提供するサイトは多くなっていますから、あなたは試験を準備するとき、復習の方法に悩んでいます。我々のCISSP資料は弊社の専門家たちによって開発されて、あなたの試験への合格を助けることができます。それに、CISSP問題集はもう更新されましたので、受験生たちの不安を削除することができます。

CISSP試験問題の継続的な刷新により、当社は大きな市場シェアを占めています。強力な研究センターを構築し、CISSPトレーニングガイドでより良い仕事をするために強力なチームを所有しています。ISCこれまで、CISSP学習教材に関する多くの特許を取得しています。一方で、当社は改修の恩恵を受けています。お客様は当社の製品を選択する可能性が高くなります。一方、私たちが投資したお金は有意義なものであり、CISSP試験の新しい学習スタイルを刷新するのに役立ちます。

**>> CISSP日本語独学書籍 <<**

## CISSP試験準備資料、CISSP試験出題傾向、CISSP試験練習問題

ISC資格試験はそんなに難しいのですか？弊社の資料を利用したら、CISSP試験は簡単になります。お客様に最高のISC問題集を入手させるために、我々は常に問題集の質を改善し、ずっと最新の試験のシラバスに応じて問題集を更新しています。我々のCISSP問題集の解答を暗記すれば、お客様は必ずこの試験に合格することができます。

CISSP試験では、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、アイデンティティとアクセス管理、セキュリティ評価とテスト、セキュリティ運用、ソフトウェア開発セキュリティなど、幅広いトピックをカバーしています。この試験は250の複数選択の質問で構成されており、テストテイカーは試験を完了するのに6時間です。認定されるには、候補者は試験に合格し、情報セキュリティの分野、または4年間の経験と大学の学位で少なくとも5年の経験を持たなければなりません。

ISC CISSP（Certified Information Systems Security Professional）試験は、情報セキュリティの分野での専門知識とスキルを検証するために設計された、世界的に認められた認定試験です。この試験は、潜在的なサイバー脅威から組織を保護するためにセキュリティプログラムの設計、実装、管理を担当する個人の能力を評価する基準として考えられています。CISSP認定は業界で高く評価され、多くの組織で世界的に認められています。

## ISC Certified Information Systems Security Professional (CISSP) 認定 CISSP 試験問題 (Q625-Q630):

**質問 # 625**
What kind of certificate is used to validate a user identity?

- A. Public key certificate
- B. Attribute certificate
- C. Root certificate
- D. Code signing certificate

**正解：A**

解説：
In cryptography, a public key certificate (or identity certificate) is an electronic document which incorporates a digital signature to bind together a public key with an identity - information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.
In a typical public key infrastructure (PKI) scheme, the signature will be of a certificate authority (CA). In a web of trust scheme, the signature is of either the user (a self-signed certificate) or other users ("endorsements"). In either case, the signatures on a certificate are attestations by the certificate signer that the identity information and the public key belong together.
In computer security, an authorization certificate (also known as an attribute certificate) is a digital document that describes a written permission from the issuer to use a service or a resource that the issuer controls or has access to use. The permission can be delegated.
Some people constantly confuse PKCs and ACs. An analogy may make the distinction clear. A PKC can be considered to be like a passport: it identifies the holder, tends to last for a long time, and should not be trivial to obtain. An AC is more like an entry visa: it is typically issued by a different authority and does not last for as long a time. As acquiring an entry visa typically requires presenting a passport, getting a visa can be a simpler process.
A real life example of this can be found in the mobile software deployments by large service providers and are typically applied to platforms such as Microsoft Smartphone (and related), Symbian OS, J2ME, and others.
In each of these systems a mobile communications service provider may customize the mobile terminal client distribution (ie. the mobile phone operating system or application environment) to include one or more root certificates each associated with a set of capabilities or permissions such as "update firmware", "access address book", "use radio interface", and the most basic one, "install and execute". When a developer wishes to enable distribution and execution in one of these controlled environments they must acquire a certificate from an appropriate CA, typically a large commercial CA, and in the process they usually have their identity verified using out-of-band mechanisms such as a combination of phone call, validation of their legal entity through government and commercial databases, etc., similar to the high assurance SSL certificate vetting process, though often there are additional specific requirements imposed on would-be developers/publishers.
Once the identity has been validated they are issued an identity certificate they can use to sign their software; generally the software signed by the developer or publisher's identity certificate is not distributed but rather it is submitted to processor to possibly test or profile the content before generating an authorization certificate which is unique to the particular software release. That certificate is then used with an ephemeral asymmetric key-pair to sign the software as the last step of preparation for distribution. There are many advantages to separating the identity and authorization certificates especially relating to risk mitigation of new content being accepted into the system and key management as well as recovery from errant software which can be used as attack vectors.
References: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw-Hill/Osborne, page 540. http://en.wikipedia.org/wiki/Attribute_certificate http://en.wikipedia.org/wiki/Public_key_certificate

**質問 # 626**
Which of the following is considered the PRIMARY security issue associated with encrypted e-mail messages?

- A. Storing attachments in centralized repositories
- B. Key distribution
- C. Scanning for viruses and other malware
- D. Greater costs associated for backups and restores

**正解：B**

解説：
Encrypted e-mail messages are e-mail messages that are protected by encryption, which is a method of transforming the plaintext into ciphertext, using a secret key and an algorithm. Encryption ensures the confidentiality, integrity, and authenticity of the e-mail messages, as only the authorized parties can decrypt and read the messages, and any modification or forgery of the messages can be detected. The primary security issue associated with encrypted e-mail messages is key distribution, which is the process of securely exchanging the secret keys between the sender and the receiver of the e-mail messages. Key distribution is challenging, as it requires a secure and reliable channel, a trusted third party, or a public key infrastructure (PKI) to ensure that the keys are not compromised, intercepted, or tampered with. If the keys are not distributed properly, the encrypted e-mail messages may not be decrypted or verified by the intended parties, or may be decrypted or forged by the unauthorized parties. Storing attachments in centralized repositories is not a security issue associated with encrypted e-mail messages, as it is a method of reducing the size and the

bandwidth of the e-mail messages, by storing the attachments in a cloud service or a file server, and sending only the links to the attachments in the e-mail messages. Scanning for viruses and other malware is not a security issue associated with encrypted e-mail messages, as it is a method of detecting and removing the malicious code that may be embedded in the e-mail messages or the attachments. Greater costs associated for backups and restores is not a security issue associated with encrypted e-mail messages, as it is a method of preserving and recovering the e-mail messages or the attachments in case of a data loss or a disaster.
References: Official (ISC)2 Guide to the CISSP CBK, Fifth Edition, Chapter 3: Security Engineering, page
105. CISSP All-in-One Exam Guide, Eighth Edition, Chapter 4: Cryptography and Symmetric Key Algorithms, page 204.

**質問 # 627**
Which of the following is the MOST appropriate action when reusing media that contains sensitive data?

- A. Sanitize
- B. Degauss
- C. Erase
- D. Encrypt

**正解：A**

解説：
The most appropriate action when reusing media that contains sensitive data is to sanitize the media.
Sanitization is the process of removing or destroying all data from the media in such a way that it cannot be recovered by any means. Sanitization can be achieved by various methods, such as overwriting, degaussing, or physical destruction. Sanitization ensures that the sensitive data is not exposed or compromised when the media is reused or disposed of. Erase, encrypt, and degauss are not the most appropriate actions when reusing media that contains sensitive data, although they may be related or useful steps. Erase is the process of deleting data from the media by using the operating system or application commands or functions. Erase does not guarantee that the data is completely removed from the media, as it may leave traces or remnants that can be recovered by using special tools or techniques. Encrypt is the process of transforming data into an unreadable form by using a cryptographic algorithm and a key. Encrypt can protect the data from unauthorized access or disclosure, but it does not remove the data from the media. Encrypt also requires that the key is securely managed and stored, and that the encryption algorithm is strong and reliable. Degauss is the process of applying a strong magnetic field to the media to erase or scramble the data. Degauss can effectively sanitize magnetic media, such as hard disks or tapes, but it does not work on optical media, such as CDs or DVDs.
Degauss also renders the media unusable, as it destroys the servo tracks and the firmware that are needed for the media to function properly.

**質問 # 628**
A federal agency has hired an auditor to perform penetration testing on a critical system as part of the mandatory, annual Federal Information Security Management Act (FISMA) security assessments. The auditor is new to this system but has extensive experience with all types of penetration testing.
The auditor has decided to begin with
sniffing network traffic. What type of penetration testing is the auditor conducting?

- A. Gray box testing
- B. Black box testing
- C. White box testing
- D. Red box testing

**正解：A**

**質問 # 629**
What is the BEST approach to anonymizing personally identifiable information (PII) in a test environment?

- A. Swapping data
- B. Randomizing data
- C. Encoding data
- D. Encrypting data

**正解：B**

**質問 # 630**
.....

もしCISSP認定試験を受験したいなら、CISSP試験参考書が必要でしょう。ターゲットがなくてあちこち参考資料を探すのをやめてください。どんな資料を利用すべきなのかがわからないとしたら、JpshikenのCISSP問題集を利用してみましょう。この問題集は的中率が高くて、あなたの一発成功を保証できますから。ほかの試験参考書より、この問題集はもっと正確に実際問題の範囲を絞ることができます。こうすれば、この問題集を利用して、あなたは勉強の効率を向上させ、十分にCISSP試験に準備することができます。

**CISSP認定デベロッパー**: https://www.jpshiken.com/CISSP_shiken.html

- CISSP日本語版復習資料 □ CISSP認定内容 □ CISSP試験解説問題 □ ☀ www.xhs1991.com □☀□にて限定無料の[ CISSP ]問題集をダウンロードせよCISSP専門知識訓練
- CISSP復習教材 □ CISSP復習時間 □ CISSP認定試験 □ 《 www.goshiken.com 》サイトで➽ CISSP □の最新問題が使えるCISSP専門知識訓練
- CISSP試験解説問題 □ CISSP試験資料 □ CISSP問題集 □ ⇛ www.xhs1991.com ⇚は、“ CISSP ”を無料でダウンロードするのに最適なサイトですCISSP日本語対策
- CISSP無料試験 □ CISSP試験解説問題 □ CISSP日本語対策 □ ウェブサイト「 www.goshiken.com 」を開き、□ CISSP □を検索して無料でダウンロードしてくださいCISSPテストトレーニング
- ISC CISSP認定試験に関連する最高な過去問問題集 □ Open Webサイト➠ www.xhs1991.com □検索➠ CISSP □無料ダウンロードCISSP無料試験
- CISSP復習資料 □ CISSP専門知識訓練 □ CISSP認定試験 □ { www.goshiken.com }で➠ CISSP □を検索し、無料でダウンロードしてくださいCISSP試験解説問題
- CISSP試験資料 □ CISSPテストトレーニング □ CISSPテストトレーニング □ ▹ CISSP ◃を無料でダウンロード“ www.passtest.jp ”で検索するだけCISSP日本語認定
- CISSP復習時間 Ⓜ CISSP認定内容 □ CISSP問題集 □ ✔ www.goshiken.com □✔□で➽ CISSP □を検索して、無料でダウンロードしてくださいCISSP専門知識訓練
- CISSP試験資料 □ CISSP無料試験 □ CISSP合格体験記 □ 【 www.passtest.jp 】で「 CISSP 」を検索し、無料でダウンロードしてくださいCISSP復習時間
- 試験の準備方法-正確的なCISSP日本語独学書籍試験-信頼的なCISSP認定デベロッパー □ 時間限定無料で使える➽ CISSP □の試験問題は□ www.goshiken.com □サイトで検索CISSP問題集
- CISSP合格体験記 □ CISSP復習教材 □ CISSP合格体験記 □ 「 www.shikenpass.com 」で使える無料オンライン版➽ CISSP □ の試験問題CISSP試験資料
- lms.skitbi-cuet.com, studyduke.inkliksites.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, mpgimer.edu.in, www.stes.tyc.edu.tw, graphyx.in, www.stes.tyc.edu.tw, cou.alnoor.edu.iq, www.stes.tyc.edu.tw, Disposable vapes

P.S.JpshikenがGoogle Driveで共有している無料の2025 ISC CISSPダンプ：https://drive.google.com/open?id=1v_xf_JOXJm31VCaJQbLzcM43tPXsJQNN