

## 分野名「04. セキュリティ」

問番	内容	解説
問040001	<ul style="list-style-type: none"> <li>●利用者IDとパスワードを用いた利用者認証の問題</li> <li>●利用者認証の仕組みについて、IDとパスワード方式、チャレンジレスポンス方式、トークン方式について検討する問題である。</li> </ul>	解答・解説
問040002	<ul style="list-style-type: none"> <li>●使い捨てパスワードの仕組みに関する問題</li> <li>●サーバへのログイン可能回数とユーザ定数Kから使い捨てパスワードを作成する方法および検証に関する問題である。</li> </ul>	解答・解説
問040003	<ul style="list-style-type: none"> <li>●共通鍵暗号化方式に関する問題</li> <li>●共通鍵暗号化方式において、DH法を使用して利用者が共通鍵を共有する手順に関する問題である。</li> </ul>	解答・解説
問040004	<ul style="list-style-type: none"> <li>●ファイアウォールのフィルタリング設定、セキュリティの問題</li> <li>●インターネット上のファイアウォールの送信元、あて先、ポート番号の条件設定、セキュリティ上のリスクの問題である。</li> </ul>	解答・解説
問040005	<ul style="list-style-type: none"> <li>●秘密鍵方式、公開鍵暗号方式に関する問題</li> <li>●秘密鍵方式・公開鍵方式を用いた通信文の暗号化、公開鍵を用いたデジタル署名、公開鍵配布に関する問題である。</li> </ul>	解答・解説
問040006	<ul style="list-style-type: none"> <li>●インターネット通信でのパケットフィルタリングの問題</li> <li>●2つのファイアウォールでDMZと社内LANに分離されたネットワークのパケットフィルタリング機能に関する問題である。</li> </ul>	解答・解説
問040007	<ul style="list-style-type: none"> <li>●社内サーバへのリモートログインと利用者認証に関する問題</li> <li>●社外端末から社内サーバにログインする際の利用者認証のためのパスワード強化方式と安全性の検討に関する問題である。</li> </ul>	解答・解説
問040008	<ul style="list-style-type: none"> <li>●複数のクライアントとサーバ間の認証システムに関する問題</li> <li>●チケット、認証子を活用し、暗号化技術と組み合わせて安全性と認証の単純化を実現した認証システムに関する問題である。</li> </ul>	解答・解説
問040009	<ul style="list-style-type: none"> <li>●インターネット利用に伴うセキュリティ事故対応に関する問題</li> <li>●インターネットを利用した会員サービス実施に伴うセキュリティ事故への対策と対応について検討する問題である。</li> </ul>	解答・解説

## 分野名「04. セキュリティ」

問番	内容	解説
問040010	<ul style="list-style-type: none"> <li>●情報セキュリティにおけるリスク管理に関する問題</li> <li>●情報資産の価値、脅威、脆弱性の基準値を使用して、機密性、完全性、可用性のリスク値を求め、リスク評価を行う問題である。</li> </ul>	解答・解説
問040011	<ul style="list-style-type: none"> <li>●ICカードを利用した入退室管理システムに関する問題</li> <li>●入退室管理システムのセキュリティ要件に従って、社員、協力社員の開発室、執務室への入退室の運用に関する問題である。</li> </ul>	解答・解説
問040012	<ul style="list-style-type: none"> <li>●IPsecを利用したVPN導入に関する問題</li> <li>●暗号化鍵の安全な交換やVPNルータの認証の仕組みを活用したIPsecを利用したVPNの導入に関する問題である。</li> </ul>	解答・解説
問040013	<ul style="list-style-type: none"> <li>●情報資産のリスクアセスメントに関する問題</li> <li>●情報資産価値、脅威、脆弱性の数値化、リスク値の算出、リスク分析の評価を行うリスクアセスメント手順に関する問題である。</li> </ul>	解答・解説
問040014	<ul style="list-style-type: none"> <li>●Webサイト構築に関連するネットワークセキュリティの問題</li> <li>●会員登録、メルマガ発行、メール伝送に関係する手続やPCのオンライン保守の外部委託時のルータの設定に関する問題である。</li> </ul>	解答・解説
問040015	<ul style="list-style-type: none"> <li>●受注管理システムのセキュリティに関する問題</li> <li>●取引先を含む受注管理システムにおいて、RPSによるプロトコル変換、脆弱性攻撃、機密性、パスワードに関する問題である。</li> </ul>	解答・解説
問040016	<ul style="list-style-type: none"> <li>●</li> <li>●</li> </ul>	解答・解説
問040017	<ul style="list-style-type: none"> <li>●</li> <li>●</li> </ul>	解答・解説
問040018	<ul style="list-style-type: none"> <li>●</li> <li>●</li> </ul>	解答・解説