情報セキュリティ	小林吉純	IJ科3年、IS科3年 IM科3年	なし

★解答注意事項

問題文の(　)に入る最も適当な1つの数値、または問題文の後に続く選択項目欄の番号を表す数字(0～9)を決め、マークシートの対応する番号のカラムの中の1つの数字を塗りつぶす(マークする)こと。なお、問題文の(　)には、マークシートのカラム番号が記入されている。例えば、(13)に対しては、そこに記入すべき数字を0～9より選び、マークシートの13番カラムの0～9の1つをマークすることにより、解答を行う。更に、数値の記入が求められている場合、不要な(　)欄には0が入るものとする。また、選択項目番号を答える場合、同じ問題中の複数の(　)に同一の選択項目番号を解答してもよい。

★マークシート記入時の注意事項

マークは黒の鉛筆ではっきり行うこと。もし、マークシートが汚れた場合は、手を上げて転記を申請すること。名前欄には自分の氏名を記入すること。学籍番号欄には学生番号を記入すること。学生番号の中で学科を表す左端の1桁(英数字)を16進数と考えて、3桁の10進数に変換し(即ち、8は008、Aは010、Bは011、Cは012)、**学生番号を8桁の番号に変換して記入**すること。例えば、「B03－777」は「01103777」となる。学籍番号欄の下部の対応数字もマークすること。**塗りつぶしが不完全だと採点不能となり、結果が0点となる**恐れがあるので、注意すること!!　なお、提出はマークシートのみとし、問題用紙は持ち帰ること。

1. 以下の不正プログラム、不正行為に対応する名称を用語欄から選び、その番号に対応するマークシートの数字をマークせよ。

(1)プログラムに寄生し、攻撃を行うと共に、他のプログラムに感染し、増殖するプログラム
(2)利用者に気付かれずに、又は承認を得ずに、個人情報を収集し、転送するプログラム
(3)単独のプログラムとして存在し、攻撃を行うと共に、コンピュータからコンピュータに感染し、増殖するプログラム
(4)有用なプログラムに見せかけて、コンピュータに侵入し、攻撃を行うプログラムであり、自己増殖は行わない。
(5)外部からの指示に応じた動作を行うプログラムであり、それに感染したコンピュータは外部から操られ、不正行為を行う。
(6)広告メールなどのように、毎日何通も送られてくる不要なメール
(7)本当の企業から送信したように見せかけたメールにより、偽のWebサイトへ誘導し、個人情報を搾取するメール

0. セキュリティホール　1. トロイの木馬　2. フィッシングメール　3. スパムメール　4. チェーンメール　5. ワーム　6. ウィルス　7. ボット　8. ワクチン　9. スパイウェア

2. 以下はパスワード等の盗難に関連する記述である。記述内容を表す名称を用語欄から選び、その番号に対応するマークシートの数字をマークせよ。

(8)パソコンやATMなどを使用している時に、パスワードや暗証番号を背後から見る。
(9)キーボードから入力された文字を記憶しておくプログラムのことで、パスワード奪取に使用される。
(10)電話や電子メールで、言葉巧みに、本人を騙し、ID、パスワードを入手する。
(11)パスワードを忘れた場合に備え、個人的な質問と解答を登録しておき、パスワード問合せ時に、その質問に正解すると、パスワードを通知してくれる機能であり、親しい友人などによって悪用される危険がある。
(12)メールソフトやWebブラウザでは、IDやパスワードをハードディスクに保存しており、利用者がこれらの一部を入力した段階で、自動で補う機能があるが、パソコンを他人が使用できれば、これらの情報が盗まれる危険がある。

0. オートコンプリート　1. なりすまし　2. ショルダハッキング　3. スキミング　4. ソーシャルエンジニアリング　5. 推測攻撃　6. 辞書攻撃　7. リマインダ　8. リメインダ　9. キーロガー

3. RSA暗号に関する以下の記述の(　)内に当てはまる数値に対応するマークシートの数字をマークせよ。
相異なる2つの素数を p=5、q=19とする。
(a) この時、k=LCM(p-1,q-1)とおくと、kの値の十の位の数字は(13)であり、一の位の数字は(14)である。従って、公開鍵 e、n のうち、e=5とすると、条件(k,e)=1を満たすので、e の値は5で問題ない。この時、n の値の十の位の数字は(15)で、一の位の数字は(16)となる。
(b) また、秘密鍵 d をed≡1 mod k に基づき、ユークリッドの互助法を適用し、計算すると、十の位の数字は(17)で、一の位の数字は(18)となる。
(c) 更に、平文 M=86 とした場合の暗号文は、十の位の数字は(19)で、一の位の数字は(20)となる。

裏面にも問題あり

4. クライアントで公開鍵、秘密鍵の鍵ペアを生成し、登録要求書内に公開鍵を格納し、それをサーバへ送信することにより、公開鍵の登録要求を行うものとする。サーバは届出のあった公開鍵に対応する秘密鍵をクライアントが所有していることを確かめたい。クライアントの秘密鍵をサーバへ渡すことなく、これを確かめる方法に関して、(　)内に当てはまる用語を用語欄から選び、その番号に対応するマークシートの数字をマークせよ。

①クライアントはクライアントの公開鍵が格納された登録要求書の(21) を(22)の(23)鍵で暗号化し、ディジタル署名を作成する。
②クライアントは登録要求書とディジタル署名をサーバへ送信する。
③サーバは登録要求書とディジタル署名を受信し、登録要求書から(24)の(25)鍵を取り出す。
④サーバは取り出した(26)鍵でディジタル署名を復号し、(27)を取り出す。そして、これを登録要求書の(28)と照合する。
⑤照合結果が(29)いれば、署名が正しいと分かるので、登録要求書内の(30)鍵に対応する(31)鍵をクライアントが所有していると判断できる。

0. 共通　1. 公開　2. 秘密　3. クライアント　4. サーバ　5. ハッシュ値　6. MAC　7. 一致して　8. 違って　9. 公開鍵証明書

5. 以下は、共通鍵暗号やハッシュによる認証方法とディジタル署名の特徴である。共通鍵暗号やハッシュによる認証方法の特徴であれば1、ディジタル署名の特徴であれば2、どちらの特徴にも当てはまる場合は3、どちらの特徴にも当てはまらない場合は4、それぞれに対応するマークシートの数字をマークせよ。

(32)送信文書の改ざん検出を行える。
(33)秘密情報を共有しないと認証が行えない。
(34) ハッシュ値に対する暗号化が必要である。
(35)認証方式に関して、事前に合意を取る必要がない。
(36)蓄積された認証情報に基づいた認証が可能である。
(37)ネットワークに秘密情報を流すことなく、認証が行える。
(38)秘密情報を共有する特定の二者間でしか、認証できない。
(39)処理時間が短いため、高速な認証情報作成、認証が可能である。
(40)認証開始時に、一般に認証側から被認証側にチャレンジが送信される。
(41)判断根拠となる認証情報をどちらが生成したかを単独では判定できない。

6. 情報技術者の責任に関する下記の記述の(　)内に当てはまる用語を用語欄から選び、その番号に対応するマークシートの数字をマークせよ。

(a) 顧客の要求に応える製品、システムを期限までに完成させることが必要。開発に際しては、高(42)、高安全性、高可用性、高速性と低(43)のバランスを顧客との間で摺り合わせることが必要。
(b) 開発に際し、知り得た顧客の情報を第三者に(44)することは厳禁。また、システムやネットワークの管理の際に、接する(45)を第三者に(46)することも厳禁。
(c) 他人のシステムに対する侵入、サービス妨害、停止などを行う(47)の(48)、配布を行ってはならない。また、受注したプログラムの中に不正を行うプログラムを仕込んではいけない。
(d) 特許権、実用新案権などの(49)やプログラム保護に使われる(50)など、他人のこれらの権利を侵害してはならない。

0. 利用者情報　1. 開発　2. 不正プログラム　3. 期限　4. 著作権　5. 工業所有権　6. 商標権　7. 価格性　8. 開示　9. 信頼性