情報セキュリティ	小林吉純	IC科3年、IS科3年 IM科3年、IN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、(8)に対しては、そこに記入すべき数字を選択項目欄の0～9より選び、マークシートの8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。学籍番号欄の1桁目にはマークシート枚数番号を記入すること。2桁目には何も記入しないこと。学籍番号欄の3桁目には学生番号の1桁目の英数字(A、B、C、Q、N、8、9)を以下のような対応する数字(1、2、3、4、5、8、9)に変換し、記述のこと。

A:1、B:2、C:3、Q:4、N:5、8:8、9: 9

学籍番号欄の4～8桁目には、学生番号の下5桁の数字を記入のこと。例えば、学生番号「Q09－123」の場合、学籍番号欄の3～8桁目は「409123」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、マークシートの裏面には何枚目であるかの番号(①、②、③)を大きく記述し、問題用紙は持ち帰ること。

マークシート1枚目

〔到達目標 a〕

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

1.1 その1

(1)強制的に広告を表示するプログラム
(2)キーボードからの入力情報を収集するプログラム
(3)Webサイトのアクセス履歴を収集するためのクッキー
(4)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

0. スパイウェア　1. アドウェア　2. キーコレクター　3. キーロガー
4. トロイの木馬　5. ワーム　6. ウィルス　7. ボット　8. トラッキングクッキー
9. コレクティングクッキー

1.2 その2

(5)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
(6)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。
(7)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
(8)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。

0. スパイウェア　1. アドウェア　2. コレクター　3. マスカレード　4. トロイの木馬
5. ワーム　6. ウィルス　7. ボット　8. スレーブ　9. スクリプト

2. 以下の攻撃等の名称を対応する用語欄から選び、その番号に対応するマークシートの数字をマークせよ。

2.1 その1

(9)侵入後の再侵入を容易にするための仕掛け
(10)システムに侵入後、管理者権限を行使し、不正行為の隠蔽などを図るツールのセット
(11)入力情報をそのまま表示する機能を持ったWebサイトを利用して、危険なプログラムを送り込む攻撃

0. システムキット　1. ツールキット　2. ルートキット
3. ツールインジェクション　4. Webサイト攻撃
5. クロスサイトスクリプティング攻撃　6. Webサイトスクリプティング攻撃
7. 踏み台　8. バックドア　9. ブラウザクラッシャー

2.2 その2

(12)大量のパケットを送信する等の手段により、システムを機能停止に追い込む攻撃
(13)Webサイトに対し、不正なデータベース命令を投入し、データベースの不正操作を行う攻撃
(14)システムのデータ領域をあふれさせ、システムの暴走や不正プログラムの実行を行わせる攻撃

0. システムオーバフロー攻撃　1. バッファオーバフロー攻撃
2. データオーバフロー攻撃　3. SQLインストラクション攻撃
4. SQLインジェクション攻撃　5. SQLスクリプティング攻撃　6. ボット攻撃
7. パケット攻撃　8. DoS攻撃　9. SoD攻撃

3. 以下の迷惑メール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。

(15)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
(16)有用なメール、重要なメールに見せかけ、転送を促すメール
(17)圧縮率が非常に高い添付ファイル付きメールであり、受信者側での解凍によりハードディスクの容量を圧迫し、パソコンの動作を不安定にするメール
(18)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. 警告メール　1. メール爆弾　2. フィッシングメール　3. チェーンメール
4. 催促メール　5. POPメール　6. HTMLメール　7. アドメール
8. スパムメール　9. スパイメール

〔到達目標 b〕

1. 以下は共通鍵暗号方式、公開鍵暗号方式の特徴である。共通鍵暗号方式の特徴であれば1 、公開鍵暗号方式の特徴であれば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。

(19) 認証に使用できる。
(20) 鍵の長さが比較的短い。
(21) 処理時間が比較的短い。
(22) 大量データの暗号化に適す。
(23) 秘密に保持する鍵の数が少ない。
(24) 鍵を秘密に配送しておく必要がある。
(25) 解読の困難さは鍵の長さに比例する。
(26) 一般に暗号アルゴリズムは非公開である。
(27) 専用ハードウェアの開発が比較的容易である。
(28) 暗号文の受信者は送信者の範囲を特定できる。
(29) 機能するためには、鍵と本人との対応を証明する機関が必要である。

裏面にも問題あり

2. 以下は共通暗号方式の適用モードの特徴を記述したものである。それぞれに対応する適用モードの組合せを選択欄から選び、その番号に対応するマークシートの数字をマークせよ。

(30) 同期式ストリーム暗号として使用できる。
(31) 自己同期式ストリーム暗号として使用できる。
(32) 暗号アルゴリズムの機能は復号しか使用しない。
(33) 暗号アルゴリズムの機能は暗号化しか使用しない。
(34) 暗号アルゴリズムの暗号化、復号の機能を使用する。
(35) 暗号文作成時や平文への変換時に、初期値を必要とする。
(36) 暗号通信時、送受信者間での鍵の事前共有は必要でない。
(37) 暗号文作成時や平文への変換時に、排他的論理和を使用する。
(38) 暗号文作成時、暗号アルゴリズムの繰り返し適用が通常必要になる。
(39) 鍵が同一の場合、同じ平文は同じ暗号文となるため、解読されやすい。
(40) 暗号文の作成プログラムと平文への変換プログラムに同一のものを使用できる。
(41) 平文の暗号化に1つ前の暗号文を使用するため、暗号化は順番に行う必要がある。
(42) 暗号文の一部が削除されたり、並び替えが行われたりしても、正しく復号できる場合がある。
(43) 平文と排他的論理和を取るデータの事前作成が可能で、暗号文作成時の処理を高速化できる。

0:何れにも該当しない、1:ECBのみに該当、2:CBCのみに該当、
3:OFBのみに該当、4:CFBのみに該当、5:ECB、CBCに該当、
6:OFB、CFBに該当、7:CBC、CFBに該当、8:CBC、OFB、CFBに該当、
9:すべてに該当

マークシート2枚目

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=3、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(1)であり、一の位の数字は(2)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(3)で、一の位の数字は(4)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(5)で、一の位の数字は(6)となる。
(c) 更に、平文 M=46 とした場合の暗号文は、十の位の数字は(7)で、一の位の数字は(8)となる。

〔到達目標 c〕

1. PKI に関する以下の記述の( )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。

PKI とは、(9)暗号方式をベースに(10)暗号方式を組み合わせ、通信相手や文書作成者の(11)、文書の(12)チェック、暗号化による文書の(13)保証などの情報セキュリティに関する機能を提供する情報基盤のことである。(14)の役割は公開鍵とその所有者との対応関係を証明する(15)を発行することであり、この対応関係の保証がなければ、PKI が成立しなくなる。

0. 共通鍵 1. 公開鍵 2. 認証 3. 公証 4. CA 5. AC 6. 秘匿性
7. 完全性 8. 公開鍵証明書 9. 所有者証明書

2. 以下はディジタル署名、メッセージ認証の特徴である。ディジタル署名の特徴であれば1 、メッセージ認証の特徴であれば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。

(16) 処理に、より時間が掛かる。
(17) メッセージ送信者を特定できる。
(18) メッセージの改ざんを検出できる。
(19) 受信メッセージの保証者を確認できる。
(20) 蓄積メッセージの保証者を確認できる。
(21) ネットワークに秘密情報が流れることがない。
(22) 送受信者間での秘密情報の共有が前提となる。
(23) メッセージを送信しなくても保証者の確認ができる。
(24) メッセージのハッシュ値に対する暗号化が必要である。
(25) メッセージと秘密情報を連結し、それに対し、ハッシュを取る。
(26) メッセージの確認には、保証者の公開鍵証明書が必要である。

3. 以下は二人の間での暗号メール、署名メールを送受信する状況を記述したものである。二人とも自分の公開鍵証明書、秘密鍵は自分のメーラに設定しているが、相手の公開鍵証明書は未設定であるとして、以下の文を手順に従って並べた場合の順序番号(1から始める)を各カラム毎にマークせよ。

(27) 共通鍵で暗号メールを復号する。
(28) 自分の署名の付いたメールを作成する。
(29) 暗号化された共通鍵を自分の秘密鍵で復号する。
(30) 共通鍵を作成し、共通鍵で暗号メールを作成する。
(31) 暗号化された共通鍵と暗号メールを相手に送信する。
(32) 相手の公開鍵証明書に基づき、メールの署名を検証する。
(33) 相手の公開鍵証明書内の公開鍵で共通鍵を暗号化する。
(34) 署名付きメール、自分の公開鍵証明書を相手に送信する。

マークシート3枚目
〔到達目標 d〕

1. 共通鍵暗号を用いて、通信相手の認証を行う以下の手順の( )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。

①認証側で(1)を生成し、被認証側へ送信
②被認証側で受信した(2)を共通鍵で(3)し、それを認証側へ送信
③認証側で受信データを共通鍵で(4)し、元の(5)と比較
④比較結果が一致していれば、認証(6)と判断

0. 平文 1. 暗号文 2. チャレンジ 3. レスポンス 4. 暗号化 5. 復号
6. OK 7. 不可 8. ハッシュ値 9. ディジタル署名

2. 以下はワンタイムパスワード方式である時間同期、カウンタ同期、チャレンジレスポンスに関する記述である。選択肢欄から、記述内容に相応しいものを選び、その番号に対応するマークシートの数字をマークせよ。

(7)なりすましを検出できる。
(8)同期がずれる恐れがある。
(9)通信相手の認証を行える。
(10)認証側でのみ、乱数を生成する。
(11)認証側と被認証側にタイマが必要である。
(12)認証側と被認証側にカウンタが必要である。
(13)ネットワークに秘密情報が流れることがない。
(14)利用者の通信メッセージの改ざんを検出できる。
(15)認証情報(パスワード、レスポンス)の盗聴を防げる。
(16)認証側と被認証側で同一の認証情報(パスワード、レスポンス)を生成する。

1:何れの方式でもない、2:時間同期方式、3:カウンタ同期方式、
4:チャレンジレスポンス方式、5:時間同期、カウンタ同期の方式に共通、
6:カウンタ同期、チャレンジレスポンスの方式に共通、
7:時間同期、チャレンジレスポンスの方式に共通、8:すべての方式に共通

3. 以下は、パスワード、ハッシュ、ディジタル署名を利用した個人認証に関する記述である。選択肢欄から、記述内容に相応しいものを選び、その番号に対応するマークシートの数字をマークせよ。

(17) 通信相手を特定できる。
(18) なりすましをされる危険が高い。
(19) 他人の秘密情報漏洩の危険が全くない。
(20) ハッシュ値に対する暗号化が必要である。
(21) チャレンジレスポンスに基づく認証である。
(22) 秘密情報を共有しないと認証が行えない。
(23) 秘密情報が推測される恐れが比較的高い。
(24) 認証情報作成や認証に必要な計算量が多い。
(25) 認証方式に関して、事前に合意を取る必要がない。
(26) 認証時には被認証側の公開鍵証明書が必要である。
(27) ネットワークに秘密情報を流すことなく、認証が行える。
(28) 認証側で秘密情報と被認証側の対応管理が必要である。
(29) 秘密情報を共有する特定の二者間でしか、認証できない。
(30) 認証情報が漏洩しても、その再利用による「なりすまし」はできない。

1:何れの認証方式でもない、2:パスワードによる認証、3:ハッシュによる認証、4:ディジタル署名による認証、5:パスワード、ハッシュによる認証に共通、6:ハッシュ、ディジタル署名による認証に共通、7:パスワード、ディジタル署名による認証に共通、8:すべての認証方式に共通