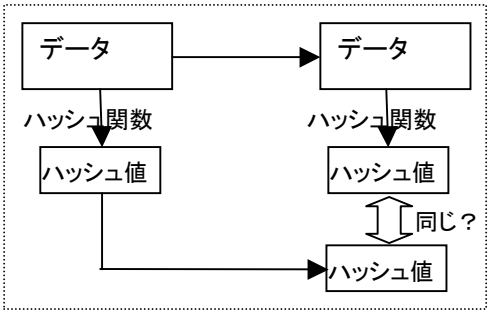
第１３回　セキュリティ（２）認証・攻撃と防御　p183～195

1） 認証とは、対象の正当性、つまり対象となるものが「本物」であることを検証・確認・(証明)する行為である。対象の1つは（　ａ　）であり、改竄されていない、つまり（　　ｂ　　）ことを確認する。 もう1つの対象は（　ｃ　　）であり、それが（　ｄ　）であることを確認する。

2） データ認証の方法として、教科書には2通り、（　ａ　）関数を用いる方法と（　ｂ　）を用いる方法が挙げてある。（ａ）関数とは、任意の大きさのデータ全体から、短い(一定の大きさの)（　ｃ　　）を計算する関数である。 右図のように、送り側であらかじめ計算した（　ｄ　）をデータと共に送り、受け側では届いた（ｄ）と、自分で受信データから計算したハッシュ値とを比較し、同じであれば（　　ｅ　　）と判断する。



この（ａ）関数は、次の4つの条件を満たさなければならない(教科書には書いていないが、自分で考えよ)

（ア） 任意の桁数のデータから、（ｆ　）の桁数のデータを出力する。

（イ） 出力されたハッシュ値から、元のデータを（　　ｇ　　）。

（ウ） 元のデータのごく一部が変更された時でも、出力されるハッシュ値は（　ｈ　　）。

（エ） 違う元データから（　ｉ　）ハッシュ値が生成される可能性はごく低い。

3） デジタル署名とは、（　ａ　）暗号を使って、送信者が（　ｂ　）鍵で暗号化し、受信者が（　ｃ　）鍵で復号し、復号できることによって（　　ｄ　　）を確認する。

4）（ユーザ認証＝物理的に「その人か？」の認証　～　たとえばログイン） ユーザ認証の方法には、特定の秘密語を知っていることを使う（　ａ　　）が広く使われているが、繰り返し利用することによって盗み取られる危険があるので、1回しか使わない（　　ｂ　　）が考案されている。（ｂ）には、時刻を利用した（　ｃ　）や、サーバー側から送られた文字列をユーザが関数で変換して送り返す（　ｄ　）がある。（ｃ）ではユーザが時刻を保持するための道具(たとえばカード電卓のような道具)を持ち、その道具の持つ時刻とサーバーの持つ時刻が同じであることを前提にして、道具が生成するパスワード文字列をサーバーに送って認証を受ける。（ｄ）ではサーバーが送った文字列を変換する関数として小さい電卓のような道具で計算する。

また、単純にユーザが物理的な鍵を持っているかどうかで認証する方式も使われており、これを（　ｅ　　）と呼ぶ。たとえば（　ｆ　）や（ｇ）が用いられる。（ｆ）には磁気ストライプが貼り付けてあり、そこに書かれた暗証データを読み取るし、（ｇ）の中にはICチップが入っており、同様にそこに書かれた暗証データを読み取ったり、また能動的な計算能力を持たせチャレンジ・レスポンスのようなことをさせる場合もある。（ｆ）や（ｇ）の場合、特別な（　ｈ　）が必要であり、コストが生じる。

5） もう1つの方法は、利用者の体の一部などを使った（　ａ　　）である。 具体的には、手の指の（　ｂ　）、 瞳の（　ｃ　）、手のひらなどの静脈のパターンなどを用いる。

（以後、教科書には書いていないが自分で考えてみよ） この方法の利点は、（　　ｄ　　）し、かつ（　　ｅ　　）。（ｄ）は、忘れたりしないし、忘れないように紙に書いて貼っておく～そのために他人に見られる～ということがない。（ｅ）は、落としたり盗まれたりすることがない。

他方、この方法の欠点は、（　ｆ　　）ことや（　ｇ　）ことが考えられる。（ｆ）ことは、万が一それを写し取られた時、具体的にはもし指紋を写し取られて指の模型を作られた時、パスワードと違って（　ｆ　　）。 特に虹彩の場合は代わりが効かない。（ｇ）ことは、たとえば指紋の場合、指を怪我して傷跡が残るとそのままでは認証できない。

6） 利用者(人間)と公開鍵との対応を保証する（　ａ　　）が考えられている。 公開鍵の持ち主が本人であることを、信頼できる（　ｂ　）が認めるという仕組である。 具体的な例として、ネットショッピングのホームページ参照の時、そのページが本当に

その持ち主の掲載したものであるという証明が欲しい。こっそりと成り済まして、クレジット番号と暗証番号をタイプインさせられたのは困る。そこで、https というプロトコルでは、（ b ）に問い合わせてそのページが本当にショッピング会社のものであるかどうかを確認できる。

7） 暗号などを用いて認証や秘匿を行っても、その他の機能からシステムへ侵入されて破壊されたり書き換えられたりするのでは、安全は保たれない。OSは外部の侵入からシステムを守る立場であり、それが正常に動作すれば安全が保たれるように作られるのだが、複雑さゆえの考え落としがある。不正にコンピュータの資源を利用したり、本来知ることができない情報を入手できたりするシステムの（ a ）を（ b ）と呼ぶ。 またこのような（ b ）を有するシステムは（ c ）を持つという。

8） セキュリティ上問題となるソフトウェアを（ a ）もしくは（ b ）と呼ぶ。 以下に代表的な種類による分類を列挙する。
有益な（＝通常の）ソフトウェアに偽装して、利用者をだまして、不正にデータを取得したりコンピュータに侵入したりするソフトを（ c ）と呼ぶ。 ユーザがよくダウンロードして利用するソフト、たとえば動画の再生ソフトやアンチウィルスソフトなどに偽装し、ダウンロードさせて実行させる。トロイの木馬の機能は、たとえば遠隔操作を受付ける、パスワードを盗んで送信する、他の特定のサイトへ接続要求を集中して送る、などが有名である。ダウンロード内容が正規のソフトにトロイの木馬を加えたものの場合、ユーザはトロイの木馬をインストールしたことに全く気付かないことがある。
コンピュータや利用者の情報を収集し外部へ送信するソフトを（ d ）と呼ぶ。 入力されたキーを記録して送信する（ e ）や、パスワード情報を読み出して送信するソフトなどがある。
コンピュータウィルスと呼ばれるのは、感染先のファイルの一部を書き換えて自分コピーを追加し（寄生し）、感染したファイルを実行したときに自分自身をコピーするコードを実行させて増殖するという、（ f ）を持つソフトである。ウィルス自身は独立して実行可能なプログラムではなくプログラム断片であり、他のファイルに感染することにより実行できる。機能は、単純にシステムを破壊するものや、上記の2つにあるようなものと同じものがある。
ワームは、ウィルスと似ているが、寄主（宿主）を必要としない、独立したプログラムである点が異なる。
ルートキットとは、プロセス・ファイルなどの資源やその動作を（診断ソフトやセキュリティソフトから）隠蔽し見えなくする。単純な例では、ファイルのリストを表示する（OSカーネルの）仕組（API）を改変して、マルウェアのファイルを表示しないようにするなど。興味ある人は、たとえば http://itpro.nikkeibp.co.jp/article/Windows/20060117/227369/ など参照。

9） 教科書には、代表的な攻撃方法を解説してある。
ソーシャルエンジニアリングとは、（ a ）によって、秘匿された情報を入手しようとする技術である。 具体的には、初期のオレオレ詐欺のように（ b ）と偽って（ c ）などする、（ d ）行為などがある。 また、ごみから情報を探したり、電話を盗聴したりするものも含まれる。 また、銀行などとほとんど同じ Web サイトを用意してユーザに誤認させ、パスワードなどを詐取する（ e ）も含まれる。
システム（ハード・OSを含めて）が正常なサービスを提供できなくする攻撃を （ f ）攻撃と呼ぶ。 インターネット上で「サイトがダウンさせられる」というニュースはこの種の攻撃の場合が多い。 攻撃は、多数の（処理能力を超えるような量の）サービス要求をシステムに送りつけて、システムが処理しきれないためにダウンする、という方法が使われる。 一般には1台の攻撃マシンからの要求では量が不足するので、ネット上の多数の攻撃マシンから同時に要求を送る（ g ）攻撃が使われる。（ g ）を送出する攻撃マシンは、マルウェアに感染したエンドユーザのPCが使われ、これらを（ h ）と呼ぶことがある。
プログラムで想定していたバッファ領域を超えて、データの書込みを行うことを（ i ）と呼ぶ。 たとえば、ネットから入力を受けて要求を処理するシステムにおいて、入力のフィールドを 20 文字とし、プログラムはバッファを 20 文字分用意するが、それに対して 100 文字書き込むとどうなるだろうか。バッファ領域の先頭から1文字ずつ順に埋めて行くので、バッファ領域が終わったその後の部分にも更に 80 文字分を書き込んでしまうだろう。この予期しない書込みによって、たとえば手続きの戻り番地を上書きするなどの操作が可能な場合があり、その時は別のプログラムへ戻って実行させることができる。 このような問題は、入力をバッファへ書き込むときに（ j ）すれば防ぐことは可能であるが、すべての場合についてこのような問題が無いことを確認するのは難しく、しばしば問題が発見され、修正プログラムが配布されている。

10） 攻撃からの防御の技術について、いくつか触れておく。
ウィルスなどのマルウェアからシステムを防御するためのソフトウェアを（　a　）もしくは（　b　）と呼ぶ。多様な製品が出回っているが、たとえばダウンロードしたファイルが（　c　）を判定するために、知られているウィルスが持つパターンとファイルとを比較し、感染しているファイルは排除する。 ウィルスは次々と新しいものが作られるので、このパターンは（　d　）しなければならない。
ネットワークとの通信の経路上に介在し、防御の機能をする装置やソフトを（　e　）と呼ぶ。 名前の通り、外からの火事を中へ引き込まないように防ぐ壁の役割をする。具体的には、通信経路上を流れる情報を（　f　）し、問題のある情報を（　g　）する。 （ e ）の設置場所は、個々のコンピュータの内部であったり、サイトの入り口（企業や大学と外部とが接続してある所）であったりする。（ e ）の実現として、IP パケットのヘッダ情報を見て通貨・遮断を決める（　h　）が広く使われている。（ h ）の利点は（　i　）であるが、柔軟な制御はできない。 また、パケットの内容を精査するタイプの（ e ）もあり、たとえばサイトの入り口に置かれ、ホームページアクセス時のダウンロードデータや、サイトに到着するメールなどのデータをすべてスキャンし、マルウェアが含まれていないか精査するものもあって、（　j　）と呼ばれることがある。
安全性が確認されていないプログラムを、外部に影響しない、閉じ込めた環境で実行させることがある。この仕組を（　k　）と呼ぶ。

≪解答≫
1） a データ　b 書き換えられていない、オリジナルと同じ、 c 利用者　d 本人
2） a ハッシュ関数　b デジタル署名　c ハッシュ値　d ハッシュ値　e 改竄されていない（書き換えられていない）
f 一定　g 復元できない（復号できない）　h 変化する（違うものになる）　i 同じ（同一の）
（注1： （イ）のことを、「一方向性」（関数）とよぶことがある。）
（注2： （エ）のことを「衝突」（コリジョン）とよぶことがある。 衝突については、元のデータが長くて、出力されるハッシュ値が短いのであるから、異なる入力に対して同じ出力が生成されることは、常にあり得る。「可能性がごく低い」というのは必ずしも正しくない。 ただ、入力データが文字列などの場合に顕著であるが、すべてのビットパターンが起こるわけではなく、ごく特定のパターンしか起こらない場合、出力が同じになることがまれであるように作れる可能性がある。いずれにせよ、衝突が起こりにくいのが望ましいことには、間違いない。）
3） a 公開鍵　b 秘密　c 公開　d 正当な送信者から送られてきたこと
（注： 秘匿したいデータの公開鍵暗号化送信と似ているのだが、鍵の使い方が異なるので、よく注意して欲しい。データ秘匿の場合は、受信者が鍵対を生成し、送信者が公開鍵を受け取って暗号化、受信者が秘密鍵で復号する。それに対して、デジタル署名では、送信者が鍵対を生成し、送信者は秘密鍵で暗号化し、受信者は公開鍵を受け取って復号する。この場合は公開鍵が公開されているので、だれでも復号できる。証明したいのは、送信者が正しい人か、ということだけであり、データは秘匿しない。）
4） a パスワード　b ワンタイム・パスワード　c 時刻同期方式　d チャレンジ・レスポンス方式
e ハードウェアキー　f 磁気カード　g ICカード　h リーダ（読み取り機）
5） a 生体認証　b 指紋　c 虹彩 （教科書には光彩と書いてあるが虹彩が正しい。目の黒いところ＝瞳ではなくて、その外側の褐色もしくは西洋人ではとび色とか青とかの部分で、この中の血管のパターン＝筋が、指紋と同じように人によって異なる）
d 記憶に頼らなくて良い　e カードなどの「もの」を持っていなくて良い　f 変更できない　g 変わってしまうことがある
6） a 公開鍵基盤　b 認証局
（注： 認証局は、現在は広く認められた私的な企業が運営しているが、一方で公的な基盤として整備すべきだという考えも強い。要するに、戸籍謄本や住民票のように役所が証明しようというものである。）
7） a 不具合　b セキュリティ・ホール　c 脆弱性
（注： システムは本来、安全に動作するように設計され・作られているはずである。それが外部からの侵入等を受けることは、本

来あるべき機能が無い「不具合」であると言える。残念ながら、複雑なOSでは多数のセキュリティ・ホールが見つかる。これは偏にOSのプログラムが複雑になり、プログラム内で、またプログラムとハードウェアの接点で、設計者が思ってもいない動作をするからである。本来は「不具合」＝欠陥なのであるから、欠陥商品として損害賠償を請求できてもよいと思うのだが、今のところはできない。）

8） a 不正ソフトウェア・悪意のあるソフトウェア、 b マルウェア

c トロイの木馬 d スパイウェア e キー・ロガー f 自己伝染機能

9） a 人を欺く社会的な手段 b 親族（息子） c 現金を振り込ませる d なりすまし（教科書参照）

e フィッシング （フィッシングという言葉は知っておいてください。 Fishing＝魚釣り＝ではなくて phishing、発音は同じ）

f サービス不能 （むしろ、「DoS 攻撃」、 Denial of Service という言葉を覚えておくこと）

g 分散サービス不能 （むしろ、「DDoS 攻撃」、 Distributed DoS という言葉を覚えておくこと）

h 踏み台、ゾンビ （悪意ある者に制御されているロボットという意味で「ボット（bot）」と呼ばれることがある）

（注： この場合、エンドユーザのPCが感染することが、単なる感染の被害者になるだけでなく、意図せずに他人への攻撃者となることを、よく認識すべきである）

i バッファ・オーバーラン j 入力の長さを数えて（チェックして）、バッファ長を超えた部分に書き込まないように

10） a ワクチン b アンチウィルスソフトウェア c ウィルスに感染していないか （ウィルスを含んでいないか）

d 常に最新のものを入手・使用

e ファイヤウォール （防火壁） f 検査、チェック g 利用者に通知したり、取り除いたり

h パケット・フィルター i 実装が容易 j 侵入検知システム（IDS、Intrusion Detection System）

k サンド・ボックス

≪情報処理技術者試験より≫

1） 入力パスワードと登録パスワードを用いて利用者を認証する方法において， パスワードファイルへの不正アクセスによる登録パスワード盗用の防止策はどれか。（基本 23 秋 42）

ア パスワードに対応する利用者 ID のハッシュ値を登録しておき，認証時に入力された利用者 ID をハッシュ関数で変換して参照パスワードと入力パスワードを比較する。

イ パスワードをそのまま登録したファイルを圧縮した状態にしておき，認証時に復元して，入力されたパスワードと比較する。

ウ パスワードをそのまま登録しておき，認証時に入力されたパスワードと登録内容をともにハッシュ関数で変換して比較する。

エ パスワードをハッシュ値に変換して登録しておき，認証時に入力されたパスワードをハッシュ関数で変換して比較する。

2） 認証デバイスに関する記述のうち，適切なものはどれか。（基本 23 春 43）

ア IEEE802.1X では，ディジタル証明書や利用者 ID，パスワードを格納する USB キーは，200k バイト以上のメモリを内蔵することを規定している。

イ 安定した大容量の電力を必要とする高度な処理には，接触型 IC カードよりも非接触型 IC カードの方が適している。

ウ 虹(こう)彩認証では，成人には虹彩の経年変化がないので，認証デバイスでのパターン更新がほとんど不要である。

エ 静電容量方式の指紋認証デバイスでは，LED 照明を設置した室内において正常に認証できなくなる可能性がある。

3） バイオメトリクス認証システムの判定しきい値を変化させるとき，FRR（本人拒否率）と FAR（他人受入率)との関係はどれか。（基本 20 春 64）

ア FRR と FAR は独立している。

イ FRR を減少させると，FAR は減少する。

ウ FRR を減少させると，FAR は増大する。

エ FRR を増大させると，FAR は増大する。

4） 情報システムへの脅威とセキュリティ対策の組合せのうち，適切なものはどれか。（基本 20 春 66）

	脅威	セキュリティ対策
ア	誤操作によるデータの 論理的な破壊	ディスクアレイ
イ	地震と火災	コンピュータ内で複数の仮想化OSを 利用したデータの二重化
ウ	伝送中のデータへの 不正アクセス	HDLC 手順の CRC
エ	メッセージの改竄	公開鍵暗号方式を応用したディジタル署名

5） 送信者から電子メール本文とそのハッシュ値を受け取り，そのハッシュ値と，受信者が 電子メール本文から求めたハッシュ値とを比較することで実現できることはどれか。受信者が送信者から受け取るハッシュ値は正しいものとする。（基本 24 春 40）

ア 電子メールの送達の確認

イ 電子メール本文の改ざんの有無の検出

ウ 電子メール本文の盗聴の防止

エ なりすましの防止

6） コンピュータウイルス対策ソフトのパターンマッチング方式を説明したものはどれか。（基本 23 秋 43）

ア 感染前のファイルと感染後のファイルを比較し，ファイルに変更が加わったかどうかを調べてウイルスを検出する。

イ 既知ウイルスのシグネチャコードと比較して，ウイルスを検出する。

ウ システム内でのウイルスに起因する異常現象を監視することによって，ウイルスを検出する。

エ ファイルのチェックサムと照合して，ウイルスを検出する。

7） ディジタル署名に用いる鍵の種別に関する組合せのうち，適切なものはどれか。（基本 22 秋 39）

	ディジタル署名の 作成に用いる鍵	ディジタル署名の 検証に用いる鍵
ア	共通鍵	秘密鍵
イ	公開鍵	秘密鍵
ウ	秘密鍵	共通鍵
エ	秘密鍵	公開鍵

8） バイオメトリクス認証には身体的特徴を抽出して認証する方式と行動的特徴を 抽出して認証する方式がある。行動的特徴を用いているものはどれか。（基本 22 秋 40）

ア 血管の分岐点の分岐角度や分岐点間の長さから特徴を抽出して認証する。

イ 署名するときの速度や筆圧から特徴を抽出して認証する。

ウ どう孔から外側に向かって発生するカオス状のしわの特徴を抽出して認証する。

エ 隆線によって形作られる紋様からマニューシャと呼ばれる特徴点を抽出して認証する。

9） 手順に示す電子メールの送受信によって得られるセキュリティ上の効果はどれか。（基本 22 秋 41）

〔手順〕

(1) 送信者は，電子メールの本文を共通鍵暗号方式で暗号化し（暗号文），その共通鍵を受信者の公開鍵を用いて公開鍵暗号方式で暗号化する（共通鍵の暗号化データ）。

(2) 送信者は，暗号文と共通鍵の暗号化データを電子メールで送信する。

(3) 受信者は，受信した電子メールから取り出した共通鍵の暗号化データを，自分の秘密鍵を用いて公開鍵暗号方式で復号し，得た共通鍵で暗号文を復号する。

ア 送信者による電子メールの送達確認

イ 送信者のなりすましの検出

ウ 電子メールの本文の改ざんの有無の検出

エ 電子メールの本文の内容の漏えいの防止

10） データの破壊，改ざんなどの不正な機能をプログラムの一部に組み込んだものを 送ってインストールさせ，実行させるものはどれか。（基本 20 秋 64）

ア DoS 攻撃　　イ 辞書攻撃

ウ トロイの木馬　　エ バッファオーバーフロー攻撃

11） 利用者認証に用いられる IC カードの適切な運用はどれか。（基本 20 秋 65）

ア IC カードによって個々の利用者を識別できるので，管理負荷を軽減するために全利用者に共通な PIN を設定する。

イ IC カードの表面に刻印してある数字情報を組み合わせて，PIN を設定する。

ウ IC カード紛失時には，新たな IC カードを発行し，PIN を設定した後で，紛失した IC カードの失効処理を行う。

エ IC カードを配送する場合には，PIN を同封せず，別経路で利用者に知らせる。

12） Web サーバが外部から侵入され，コンテンツが改ざんされた。 その後の対応の順序のうち，適切なものはどれか。（基本 20 秋 67）

①	サーバ，IDS（Inttsion Detection System），ファイアウォールの各ログを解析し，不正アクセス手法，影響範囲，侵入経路を特定する。
②	システムを再構築し，最新のパッチやセキュリティ設定情報を適用する。
③	サーバをネットワークから切り離す。
④	ネットワークに接続後，しばらく監視する。

ア ①→②→③→④　　イ ①→③→②→④

ウ ②→③→①→④　　エ ③→①→②→④

13） ファイアウォールのパケットフィルタリング機能に関する記述のうち，適切なものはどれか。（基本 16 秋 72）

ア インターネットから受け取ったパケットに改ざんがある場合は修正し，改ざんが修正できない場合には，ログを取って内部ネットワークへの通過を阻止する。

イ インターネットから受け取ったパケットのヘッダ部分及びデータ部分に，改ざんがあるかどうかをチェックし，改ざんがあった場合にはそのパケットを除去する。

ウ 動的に割り振られた TCP ポート番号をもったパケットを，受信側で固定値の TCP ポート番号をもったパケットに変更して，内部ネットワークへの通過を許可する。

エ 特定の TCP ポート番号をもったパケットだけに，インターネットから内部ネットワークへの通過を許可する。

14） フィッシングの手口に該当するものはどれか。（基本 18 秋 66）

ア Web ページに入力した内容をそのまま表示する部分がある場合，ページ内に悪意のスクリプトを埋め込み，ユーザとサーバに被害を与える。

イ ウイルスに感染したコンピュータを，インターネットなどのネットワークを通じて外部から操る。

ウ コンピュータ利用者の IP アドレスや Web の閲覧履歴などの個人情報を，ひそかに収集して外部へ送信する。

エ 電子メールを発信して受信者を誘導し，実在する会社を装った偽の Web サイトにアクセスさせ，個人情報をだまし取る。

≪解答≫

1） エ　ア： ハッシュ関数では衝突があるので不十分　イ： 圧縮だけでは復元されて盗まれてしまう　ウ： 盗まれてしまう

2） ウ　ア： 802.1X は LAN 接続時に端末を認証するための規格　イ： 電力を供給するためには接触型の方が適している
エ： 静電型の場合、照明には関係ない

3） ウ　バイオメトリクス認証（生体認証）では、必ずしもいつも正しく認証できるとは限らず、失敗することもある。それに関する指標として、FRR（本人拒否率）と FAR（他人受入率）がある。 本人拒否率は、正しい本人であるのに、認証システムが拒否する場合の（全体に対する）割合、 他人受入率は、他人であるのに、認証システムが本人だと思って受け入れてしまう場合の（全体に対する）割合である。 いずれも小さい方が良いのだが、一般に、条件を厳しくすると他人受入率は下がるが本人拒否率が上がり、条件を緩くすると本人拒否率は下がるが他人受入率が上がってしまう。

4） エ

ア： ディスクアレイは複数のディスクに並列にデータを書込み、故障などに対応するが、利用者の誤操作による破壊を復旧することはできない。

イ： 地震や火災に対応するためには、別の場所に保管しなければならない。同じ場所では同じように被害を蒙る。

ウ： HDLC の CRC（巡回冗長検査）は、通信の途中でデータが壊れていないか検査する仕組（パリティ検査の拡張）であり、伝送中の不正アクセスは検知できない。

5） イ 送信者からメールの本文から求めたハッシュ値が、受信者が受け取ったメールの本文から求めたハッシュ値と異なっていた場合、送信時のメールの本文と受信時のメールの本文が異なっていることになり、「メールが改ざんされている」ことになる。

6） イ

ウイルス定義ファイルは、コンピュータウイルスに感染したファイルやワームプログラムの特徴を収録したファイルである。ウイルス対策ソフト（ワクチンソフト）がコンピュータウイルスやワームを検出する時に使用するファイルである。 コンピュータウイルス対策ソフトのパターンマッチング方式は、既知ウイルスのシグネチャコード（プログラムが持っている特有のコード）と比較してウイルスを検出する方式である。

7） エ 送信者は鍵対を作成し公開鍵を公開する。送信者は電文を秘密鍵で暗号化して送り、受信者は公開鍵で復号する

8） イ バイオメトリクス認証システムとは、顔や声紋、瞳の虹彩による個人認証システムである。 行動的特徴を抽出して認証する方式は、イの「署名するときの速度や筆圧から特徴を抽出して認証する」 方式である。

9） エ 本番の電文は共通鍵暗号で送るが、その（共通）鍵のみを、公開鍵暗号方式で交換する。 公開鍵暗号方式で、次に使う共通鍵を秘密裏に送ることができ、その鍵を使って共通鍵暗号で電文を送っている。従って、電文の秘匿ができる。

10） ウ イの「辞書攻撃」は、パスワードを知るために、辞書に載っている単語を片端から試すこと、 またスパムメール送信者が宛先アドレスとして辞書に載っている単語を片端から試すこと。

11） エ PIN（Personal Identification Number）は、クレジットカードやキャッシュカードの暗証番号で、カード所持と暗証番号有無でユーザを認証する。

ア：誤り 全利用者に共通な PIN を設定することは、危険である。

イ：誤り 数字情報を組み合わせて、PIN を設定するのは安全上問題である。

ウ：誤り IC カード紛失時には、まず、カードの失効処理を行う。

12） エ Web サーバが外部から侵入された場合の対応として、

外部からの侵入を防ぐために、まず、 ③「サーバをネットワークから切り離す」

次に、侵入者、侵入経路を特定するために、①「各ログを解析する」

セキュリティホールを塞ぐために、 ②「最新のパッチやセキュリティ設定情報を適用」

そのあと、 ④「ネットワークに接続し、しばらく監視する」

13） エ

ア： ファイアウォールのパケットフィルタリング自体に改ざんをチェックする機能はない。 他のセキュリティー手段によって防止を図るべきである。但し、ログを取ることは可能である。

イ： 同上

ウ：ファイアウォールに、動的に割り振られた TCP ポート番号をもったパケットを 受信側で固定値の TCP ポート番号をもったパケットに変更して、内部ネットワークへの通過を 許可する機能（ IP マスカレード機能）を持つが、これはパケットフィルタリングとは異なる。

14） エ フィッシングは、銀行などの金融機関を装った偽の電子メールを発信して、 受信者を誘導し、実在する会社などを装った偽の Web サイトにアクセスさせ、 暗証番号やクレジットカード番号などの個人情報をだまし取る手口である。