情報：ネットワーク, セキュリティ　練習問題　1年　　組　　番 氏名

問　空欄を埋めよ。

1. 世界中にある多数のネットワークをつなげ、世界規模に広がったものを(1)という。(1)に接続するためには(2)と呼ばれる接続業者と接続契約を結ぶ必要がある。ネットワークにおける伝送速度は(3)という単位で表される。学校などの建物の中や一定の区域内のネットワークを(4)といい、それよりも広域のものを(5)という。
2. インターネットは1969年にアメリカの国防総省(国防省)がはじめたARPANETが原型である。ARPANETは(6)交換方式という通信技術を採用した。(6)交換方式では、データを(6)という単位に分割して送信をするため、複数のユーザで一つの回線を共有できる。それ以前は、回線を確保してから伝送を行う(7)方式であった。
3. コンピュータネットワークで通信を実現するための約束事を(8)という。インターネットでは、データの送受信に(9)と呼ばれるプロトコル群が使われ、コンピュータには、ネット上の住所に相当する(10)が割り当てられる。(10)は、各(11)ビットの４つの数字と、境目を意味するピリオドで表記する。しかし、Webページを閲覧するときには、数字の列である(10)ではなく(12)でWebページのあるサーバの場所を指定することが多い。そのほうが人にとって分かりやすいからであるが、(10)と(12)の対応をデータベースとして持つ(13)サーバがネットワーク上に必要となる。
4. 例えばWebページのURLがhttp://www.kantei.go.jpの場合、末尾のjpの部分を(14)ドメインという。また、このURLにおいてコンピュータ名は(15)である。Webページを閲覧するときは(16)というプロトコルを、メールの送信には(17)、受信には(18)というプロトコルを利用する。
5. 悪意をもって作られたソフトウェアを(19)と呼び、他のプログラムに寄生するものが(20)、単独のプログラムが(21)である。これらは一般に、自己伝染機能、潜伏機能、発病機能をもつものが多いが、例えばスパイウェアは伝染(増殖)しない場合が多い。
6. 次のア.と イ.は暗号化技術に関する説明である。

ア．AとBが公開鍵暗号方式で暗号化された情報のやり取りをする場合、最初にAからB宛てに情報を発信するのであれば、その情報は(22)を利用して暗号化したものであればよい。また、暗号化されたBの返信メールをAが読むためには(23)で復号することになる。また、公開鍵暗号方式をAの電子署名(ディジタル署名)として用いる場合、Aは(24)を用いて暗号化すればよい。

イ．AとBがハイブリッド暗号方式によって暗号化された情報のやり取りをする場合、最初にAからB宛てに情報を発信するのであれば、(25)を利用して暗号化する。そしてその後BからA宛に情報を発信する場合は(26)を使い、さらにその後のAからBへの返信は、(27)を使用することになる。このしくみは(28)等と呼ばれて電子商取引においても使用されており、運営者の電子署名が偽造でないことを証明するために(29)が(30)を発行する。

(1)	インターネット
(2)	プロバイダ（ISP）
(3)	bps
(4)	LAN
(5)	WAN
(6)	パケット
(7)	回線交換
(8)	プロトコル（通信規約）
(9)	TCP/IP
(10)	IPアドレス
(11)	8
(12)	ドメイン名
(13)	DNS
(14)	トップレベル
(15)	www
(16)	HTTP
(17)	SMTP
(18)	POP（又はPOP3), IMAP
(19)	マルウェア
(20)	コンピュータウイルス
(21)	ワーム
(22)	Bの公開鍵
(23)	Aの秘密鍵
(24)	Aの秘密鍵
(25)	Bの公開鍵
(26)	共通鍵
(27)	共通鍵
(28)	SSL/TLS
(29)	認証機関，認証サーバ，認証局
(30)	電子(ディジタル)証明書