情報ネットワーク基礎　後期期末テスト (斉藤)　番号：
3EI　(1/2) 2018/2/5(月)　氏名：

1　穴埋め問題 (max25)

以下の説明の下線部に相応しい単語を単語群から選び答えよ。単語群に無いものは、適切な単語を答えよ。(a)〜(l)× 2,(m)×5

1. aa@foo.jp さんが自宅の自分の PC から bb@bar.jp さん宛にメールを出す場合、aa さんの PC から foo.jp のメールサーバにプロトコル (a)__________でメールが送られる。foo.jp のメールサーバは、bb さんのメールアドレスの bar.jp の部分を、(b)__________に問い合わせ、求まった IP アドレスのメールサーバに接続し、プロトコル (c)__________でメールを送り、メールはユーザ名毎に保存される。

   bb さんは、メールを読むときには自分のメールサーバに、(d)__________や (e)__________のプロトコルでメールを読む。

2. 公開鍵暗号を用いた通信では、データを暗号化するための (f)__________と、データを復号するための (g)__________を用いて通信を行う。クライアントは、サーバから (f) を取得し、乱数をもとに作られる (h)__________を、(f) で暗号化してサーバに送る。サーバは、(g) を用いて (h) を復号する。この後クライアントとサーバは、(h) を用いて暗号化通信を行う。

3. 組織内のコンピュータを守るためインターネットと接続する場所には、(i)__________が設置される。(i) は、通過するパケットの送信元の (j)__________ や接続先の (k)__________ を確認し、攻撃目的のパケットは廃棄する。

   例えば、組織内の Web サーバだけをインターネットに公開し、その他のプロトコルを利用禁止にするのなら、インターネットからのパケットで (k) の番号が (l)__________のパケットを廃棄する。

4. ぜいじゃくせいを漢字 3 文字で書け。(m)_____

単語群：

公開鍵, 共通鍵, 生体認証鍵, 土佐鍵, 秘密鍵, ディンプル鍵, シーザ暗号, AUTH, DHCP, DNS, ECHO, FTP, HTTP, HTTPS, IMAP, POP, SNMP, SMTP, SSH, TELNET, 7, 22, 25, 80, 110, 143, 177

2　説明問題 (25)

http://www.ei.fukui-nct.ac.jp/~t-saitoh/index.html といった URL が与えられて、ブラウザでページが閲覧できるまでの仕組みを説明せよ。

情報ネットワーク基礎　後期期末テスト (斉藤)　番号：
3EI　(2/2) 2018/2/5(月)　氏名：

3　対応付け問題 (3x8)

(a)-(d) と最も関係のある単語の欄に、記号を埋めよ。

1. (a) すべての文字の組み合わせでパスワードを試す攻撃
   (b) ポート番号を変えながら接続を試行する攻撃
   (c) bot 化された大量のパソコンから同時にサーバへの接続を行う攻撃
   (d) ホスト名の問い合わせに間違った IP アドレスを答えさせる攻撃

   DNS ポイズイング (_____), ブルートフォース攻撃 (_____),

   分散 DoS 攻撃 (_____), ポートスキャン (_____)

2. (a) IP ネットワークで、ノードまでの経路情報を調べるコマンド
   (b) IP ネットワークで、ノード到達性を調べるコマンド
   (c) 暗号や認証の技術を利用して安全にリモート接続するコマンド
   (d) ドメイン名や IP アドレスの対応付けを調べるコマンド

   ping(_____), nslookup(_____), traceroute(_____), slogin(_____)

4　説明問題 (26)

OS やソフトウェアの更新をしない場合の (1) 危険性と (2) 対策を、(3) バッファオーバーフロー, (4) ウィルス対策ソフト, (5) ゼロデイ攻撃の用語を交えて説明せよ。