問１　a　オ　　b　キ　　c　ア

〔解説〕a　問題文より，秘密の共通かぎの共有（オ）である。

b　α＝5のべき乗をp＝7で割ったときの余りを求めてみると，

べき乗	余り
5^1＝5	5
5^2＝25	4
5^3＝125	6
5^4＝625	2
5^5＝3125	3
5^6＝15625	1

これより，X_Aは余りがY_A＝6のときの指数値であるから3，X_Bは余りがY_B＝3のときの指数値であるから5であることがわかる。

よって，K＝3^3 mod 7＝6^5 mod 7＝6（キ）となる。

c　暗号文の傍受から共通かぎを見つけられることを防ぐには，共通かぎを頻繁に変更し，暗号文が手掛かりとなりにくいようにするのが最も有効である。よって，正解は（ア）となる。

問２　a　カ　　b　ア　　c　イ

〔解説〕ログイン可能回数Mが3回，定数Kが5の場合，以下のようにしてログイン管理を行う。

①1回目のパスワードは，otp(3)＝hash(hash(hash(5)))
サーバはこれを保持しておく。

②2回目のパスワードは，otp(2)＝(hash(hash(5))
サーバはこれをハッシュ化し，保持しておいたotp(3)と比較する。
hash(otp(2))がotp(3)＝hash((hash(hash(5)))と等しければ許可
サーバはこれを保持しておく。

③3回目のパスワードは，otp(1)＝hash(5)
サーバはこれをハッシュ化し，保持しておいたotp(2)と比較する。
hash(otp(1))がotp(2)＝(hash(hash(5))と等しければ許可

a　利用者がパスワードとしてクライアントPCに入力するものはotp(n)であるから，正解は（カ）となる。

b　サーバと使い捨てパスワード生成装置にあるものはhashであるから，正解は（ア）となる。

c　利用者本人だけが知る情報で，クライアントPC，ネットワーク上のメッセージ及びサーバに存在しないものは，定数Kであるから，正解は（イ）となる。

問３　a　キ　　b　ウ　　c　ケ　　d　ケ

〔解説〕a，b　X社のサーバはポート番号が1024，1025であるため，上段がY社のパソコンからX社のサーバへのアクセス設定であることがわかり，

aはY社のパソコンのIPアドレス　100.1.1.1：101.1.1.2　（キ）

bはX社のデータ転送用サーバ　　100.1.1.12　（ウ）

となる

c　X社のサーバのポート番号であるから，

1024：1025　（ケ）

となる

d　下段はX社のサーバからY社のパソコンへのアクセス設定であるから，cと同様に

1024：1025　（ケ）

となる

問４　**設問1**　a　エ　　b　イ　　c　エ　　d　エ　　**設問2**　ウ，エ

〔解説〕**設問1**　a　問題文(2)より，メールサーバは社外とのメールの送受信を行う。社外からメールサーバへのメール受信は設定されているが，メールサーバから社外へのメール送信が設定されていない。よって，メールサーバ（エ）が正解となる。

b　メール送信で使用されるSMTPのポート番号であるから，25（イ）である。

c　問題文より，管理用PCからは，メールサーバを介した外部とのメール送受信が可能である。管理用PCからメールサーバへのログイン，管理用PCからメールサーバへのメール送信は設定されているが，メールサーバからのメール受信が設定されていない。よって，メールサーバ（エ）が正解となる。

d　メール受信で使用されるPOP3のポート番号であるから，110（エ）である。

設問2　ア　データの盗聴や改ざんはパケットの中身に対して行われるため，パケットフィルタリングでは防げない

イ　SQLインジェクション攻撃は，不正なSQL文を送信し，データベースに対して盗聴や改ざんを行う攻撃方法であり，データの中身をチェックできないパケットフィルタリングでは防げない

ウ　パケットフィルタリングでポート番号を設定することにより防ぐことができる

エ　パケットフィルタリングで送信元，あて先を設定することにより防ぐことができる

オ　パケットフィルタリングでは，ファイルの中身をチェックしないため，メールによる社内からのファイル流出を防ぐことはできない

よって，正解は（ウ），（エ）となる。

問５　**設問１**　a　ウ　　b　カ　　c　ケ　　**設問２**　オ　　**設問３**　エ

〔解説〕**設問１**　サブネットマスクが 255.255.255.0 であることから，同じＬＡＮ内のパソコンやサーバのＩＰアドレスは上位２４ビットが同じでなければならない。

a　ルータＥ及びルータＧの基幹ＬＡＮ側のＩＰアドレスが 172.16.1.10 であることから，（ウ）が正解となる。

b　ルータＥのＹ部門ＬＡＮ側のＩＰアドレスが 172.16.10.1 であることから，（カ）が正解となる（172.16.10.255（キ)は，ブロードキャストアドレスなので使用不可）

c　ルータＧのＺ部門ＬＡＮ側のＩＰアドレスが 172.16.20.1 であることから，（ケ）が正解となる（172.16.20.255（コ)は，ブロードキャストアドレスなので使用不可）

設問２　社内の異なるサブネット及び社外へのデータ送信はルータに中継を依頼する。また，社内のＷｅｂサーバへのアクセスはプロキシ機能を使用しないから，（オ）が正解となる。

設問３　ｐｉｎｇコマンドの応答より接続は確立していることがわかる。したがって，ＦＴＰのポート番号が関門サーバで通過不能に設定されていると考えられ，（エ）が正解となる。

問６　**設問１**　a　カ　　b　エ　　設問２　c　ア　　d　エ　　e　ア

〔解説〕**設問１**　a　英小文字２６文字からなる８文字のパスワードの総数は，

26^8通り

英小文字２６文字からなる１０文字のパスワードの総数は，

26^{10}通り

８文字のパスワードを総当たり方式で発見する時間を１とした場合の１０文字でかかる時間は，

$26^8 / 26^{10} = 26^2 = 676$　（カ）

b　英小文字と英大文字５２文字からなる８文字のパスワードの総数は，

52^8通り

かかる時間は，$52^8 / 26^8 = (26 \times 2)^8 / 26^8 = 2^8 = 256$　（エ）

設問２　c　通信経路上で通信内容が盗聴された場合，

方式１：利用者ＩＤとパスワードを利用して不正ログインが可能

方式２：通信経路上にはパスワードが流れておらず，パスワードがわからなければｈ(ｐ，ｃ)を計算することができないので，不正ログインは不可

方式３：パスワードはわかるが，そのパスワードは１度しか使えないので，次回からの不正ログインは不可

よって，正解は（ア）となる。

d　キーボード入力を読み取った場合，

方式１：利用者ＩＤとパスワードを利用して不正ログインが可能

方式２：端末のキーボードから入力されたパスワードを使って不正ログインが可能

方式３：端末のキーボードから入力されたパスワードがわかっても，そのパスワードは１度しか使えないので，次回からの不正ログインは不可

よって，正解は（エ）となる。

e　不正なサーバでログイン操作を行った場合，

方式１：利用者ＩＤとパスワードを利用して不正ログインが可能

方式２：不正なサーバから送信したチャレンジに対するレスポンスを取得できるが，レスポンスは毎回サーバから送信されるチャレンジによって計算されるので，今回取得したレスポンスの再利用はできず，不正ログインは不可

方式３：パスワードはわかるが，そのパスワードは１度しか使えないので，次回からの不正ログインは不可

よって，正解は（ア）となる。

問７　a　ウ　　b　エ　　c　イ　　d　イ

〔解説〕a　クライアントＣは暗号化されたＴＩＣＫＥＴ$_{CT}$をそのままチケット発行サーバＴに送信し，チケット発行サーバＴが復号するのだから，（ウ）が正解となる。

b　ｅｎｃ(ＡＵＴＨ$_{c1}$)とｅｎｃ(ＩＤ$_S$)はクライアントＣが暗号化を行っており，クライアントＣ用いることのできる鍵は，通信②で送られたＫＥＴ$_{CT}$である。よって，正解は（エ）となる。

c　クライアントＣは暗号化されたＴＩＣＫＥＴ$_{CS}$をそのままＡＰサーバＳに送信し，ＡＰサーバＳが復号するのだから，（イ）が正解となる。

d　ｅｎｃ(ＡＵＴＨ$_{c2}$)はクライアントＣが暗号化を行っており，クライアントＣ用いることのできる鍵は，通信④で送られたＫＥＴ$_{CS}$である。よって，正解は（イ）となる。