問 1　暗号通信に関する次の記述を読んで，設問に答えよ。

安全でない通信経路を利用する２者が，秘密の共通かぎを安全に共有する方式としてDiffie-Hellman法（以下，ＤＨ法という）が知られている。ＤＨ法で利用者Ａと利用者Ｂが共通かぎＫを共有するまでの手順は，次のとおりである。

(1) 素数ｐと，ｐよりも小さいある自然数αが公開されていて，利用者Ａと利用者Ｂがともに知ることができる。

(2) 利用者Ａは，ｐよりも小さい任意の自然数X_Aを選び，秘密かぎとして保持するとともに，次の式で得られる公開かぎY_Aを利用者Ｂに送る。

$$Y_A = \alpha^{X_A} \bmod p$$

ここで，ｘ ｍｏｄ ｙは整数ｘを整数ｙで割った余り（剰余）である。

(3) 利用者Ｂは，ｐよりも小さい任意の自然数X_Bを選び，秘密かぎとして保持するとともに，次の式で得られる公開かぎY_Bを利用者Ａに送る。

$$Y_B = \alpha^{X_B} \bmod p$$

(4) 利用者Ａは，利用者Ｂの公開かぎY_Bを使って，次の式によって共通かぎＫを得る。

$$K = Y_B^{X_A} \bmod p$$

(5) 利用者Ｂは，利用者Ａの公開かぎY_Aを使って，次の式によって利用者Ａと同じ共通かぎＫを得る。

$$K = Y_A^{X_B} \bmod p$$

ＤＨ法によるかぎ共有を利用して，図に示すように，安全でない通信経路を利用する２者間で機密情報を送信する仕組みを作る。まず，利用者Ａと利用者ＢはＤＨ法を使って，共通かぎＫを共有する。次に，利用者Ａは平文を共通かぎＫを使って暗号化して送信する。利用者Ｂは受信した暗号文を共通かぎＫを使って復号して，元の平文を得ることができる。

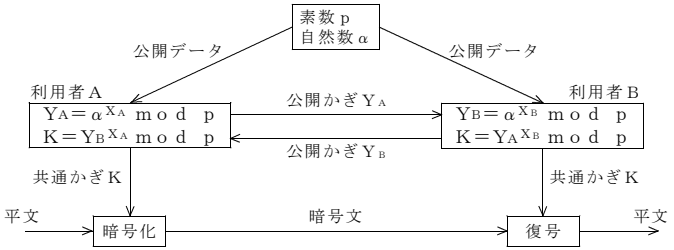


図　ＤＨ法を使った機密情報の通信

設問　次の記述中の［　　］に入れる正しい答えを，解答群の中から選べ。

ＤＨ法は，目的が［ a ］に限定されたアルゴリズムであるが，この方式の安全性はほかの公開かぎ暗号と同じく計算の一方向性に基づいている。すなわち，ＤＨ法において，素数ｐの値が十分に大きい場合，秘密かぎから公開かぎを求めるのは容易であるが，公開かぎから秘密かぎを求めるのは非常に困難である。

反対に，素数ｐの値が小さい場合には，かぎの値が小さくなるので公開かぎから秘密かぎを短時間で求めることも可能であり，安全性に問題がある。例えば，利用者Ａと利用者Ｂが使う通信経路上に通信を傍受している第三者Ｃがいて，公開されている素数ｐが７，αが５であることに加え，利用者Ａが送った公開かぎY_Aが６，利用者Ｂが送った公開かぎY_Bが３であることを知ったとする。このとき，共通かぎＫの値は，［ b ］であることが容易に分かる。

また，ＤＨ法は，通信経路上の第三者Ｃが，利用者Ａから送られる情報を，にせの情報にすりかえて利用者Ｂに送信する中間者攻撃に対して，弱いことが知られている。中間者攻撃を防ぐためには公開かぎに信頼できる第三者によるディジタル署名をつけるなどの対策が必要である。さらに，第三者Ｃが暗号文を傍受してそれを手掛かりとして共通かぎＫを見つけるリスクもあるので，継続的な通信の安全性を高めるための対策として，共通かぎＫの値が十分に大きいものを使うだけでなく，［ c ］も有効である。

a，ｃに関する解答群

ア　共通かぎＫの更新間隔の短縮　　イ　公開かぎY_A，Y_Bの交換回数の削減
ウ　公開かぎの交換　　エ　秘密かぎによる情報の復号
オ　秘密の共通かぎの共有　　カ　より大きな値の素数ｐの使用

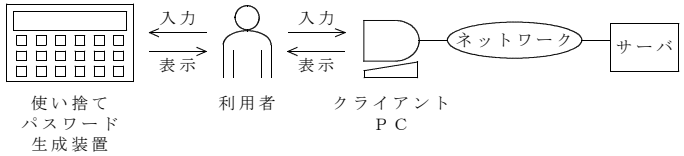
ｂに関する解答群

ア　０　　イ　１　　ウ　２　　エ　３　　オ　４　　カ　５　　キ　６

a		b		c	

問２　サーバへのログイン管理に関する次の記述を読んで，設問に答えよ。

使い捨てパスワード（One-Time Password：ＯＴＰ）の仕組みを応用して作られたログイン管理システムである。



〔ログイン管理システムの説明〕

サーバへのログイン可能回数Ｍと定数Ｋを決定し，Ｍ個の有効な使い捨てパスワードを使用する。残りのログイン可能回数がｎのときの使い捨てパスワードｏｔｐ(ｎ)には，一方向性関数ｈａｓｈを用いて，次式で得られる値を用いる。

$$otp(n) = \overbrace{hash(hash(\cdots hash}^{n\text{回}}(K)\cdots))$$

(1) 使い捨てパスワード生成装置

利用者が，使い捨てパスワードをすべて記憶し，管理することは困難なので，定数Ｋと残りのログイン可能回数ｎから使い捨てパスワードを生成し，表示する携帯式の使い捨てパスワード生成装置を用いる。

第１回目のパスワード生成時はｎ＝Ｍで，パスワードを生成するたびにｎを１ずつ減らし，最後のパスワード生成時は，ｎ＝１となる。

(2) 利用者

利用者は，Ｋを使い捨てパスワード生成装置に入力し，表示された使い捨てパスワードを，サーバへのログインパスワードとしてクライアントＰＣに入力する。

(3) サーバ

サーバは，次の二つを保持する。

①使い捨てパスワード生成装置と同じ一方向性関数ｈａｓｈ

②パスワード検査に用いるために，利用者が，直前の許可されたログインで使ったパスワード
ｏｔｐ(ｎ＋１)

サーバでのパスワード検査は，ログイン時にクライアントＰＣからサーバへ送られてきたパスワードｏｔｐ(ｎ)に，ｈａｓｈを１回適用し，ｈａｓｈ(ｏｔｐ(ｎ))を得て，それがサーバの保持しているｏｔｐ(ｎ＋１)と一致するかどうかで行う。一致すればサーバは，ログインを許可する。

サーバは，保持しているｏｔｐ(ｎ＋１)を次回の検査用に更新する必要がある。このためには，クライアントＰＣから送られてきた使い捨てパスワードの値ｏｔｐ(ｎ)で置き換えればよい。

図にログイン管理の流れを示す。ここでは，サーバには，利用者のｏｔｐ(ｎ)を受け入れる準備として，ｏｔｐ(ｎ＋１)が保持されているものとする。また，この図では，時間は上から下に向かって進むように表現されている。

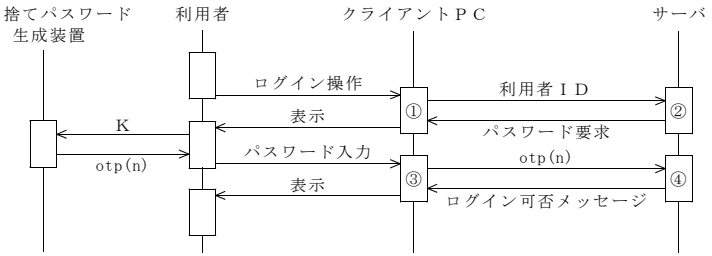


図　ログイン管理の流れ

〔図中の主な処理の説明〕

①利用者ＩＤによってサーバにログイン操作を行う。

②パスワードを要求する。

③使い捨てパスワードｏｔｐ(ｎ)をサーバへ送る。

④受け取ったｏｔｐ(ｎ)にｈａｓｈを適用し，ｈａｓｈ(ｏｔｐ(ｎ))を得る。利用者ＩＤごとに保存していたｏｔｐ(ｎ＋１)と比較する。一致すれば，ログインを許可し，受け取ったｏｔｐ(ｎ)を次回のパスワード検査用に保持する。一致しなければ，ログインを拒否する。

設問　このログイン管理に関する次の記述中の［　　］に入れる正しい答えを，解答群の中から選べ。

利用者がパスワードとしてクライアントＰＣに入力する［ a ］は，ネットワーク上の通信メッセージにも含まれる。しかし，［ a ］は，ログイン許可と同時に無効なパスワードとなるので，これを盗聴してその後で使用しても，サーバにログインすることはできない。

サーバが保持する使い捨てパスワードｏｔｐ(ｎ＋１)は，使用済みの無効なパスワードなので，これを不正に入手して使用しても，サーバにログインすることはできない。また，ｏｔｐ(ｎ＋１)とｈａｓｈを不正に入手したとしても，ｈａｓｈの一方向性の特徴から，これらを基に，未使用の使い捨てパスワードを得ることは極めて困難である。

このログイン管理の仕組みで，不正アクセスの危険性が大きいのは，［ b ］と［ c ］の両方が不正に入手，使用された場合である。

このうち，［ b ］は，サーバと使い捨てパスワード生成装置にある。サーバには，セキュリティ強化のための既存の手段を講じることができるが，使い捨てパスワード生成装置は，別の利用者も所有しているので，その不正使用及び盗難の危険性は比較的高い。

［ c ］は，クライアントＰＣ，ネットワーク上の通信メッセージ及びサーバには一時的にも存在しない情報なので，これらから盗まれる危険性はない。また，［ c ］は，利用者本人だけが知る秘密情報である。

解答群

ア　ｈａｓｈ	イ　Ｋ	ウ　Ｍ	エ　ｎ
オ　ｏｔｐ(Ｍ＋１)	カ　ｏｔｐ(ｎ)	キ　利用者ＩＤ	

a		b		c	

問３　コンピュータネットワークのアクセス制御に関する次の記述を読んで，設問に答えよ。

Ｘ社では，社内及び関連会社との通信にネットワークを使用している。Ｘ社のＬＡＮ構成を図に示す。通信プロトコルはＴＣＰ／ＩＰを用いており，図中の数字は，ＩＰアドレスを表している。このＩＰアドレスは，架空のものとする。

関連会社との接続に際して，セキュリティ上の配慮から，関門ルータを設置してある。関門ルータは，ルータを通過するすべてのパケットの内容を検査し，設定された条件に合わないものを破棄する機能をもつ。関門ルータに設定する条件は，設定テーブルにあらかじめ登録しておく。

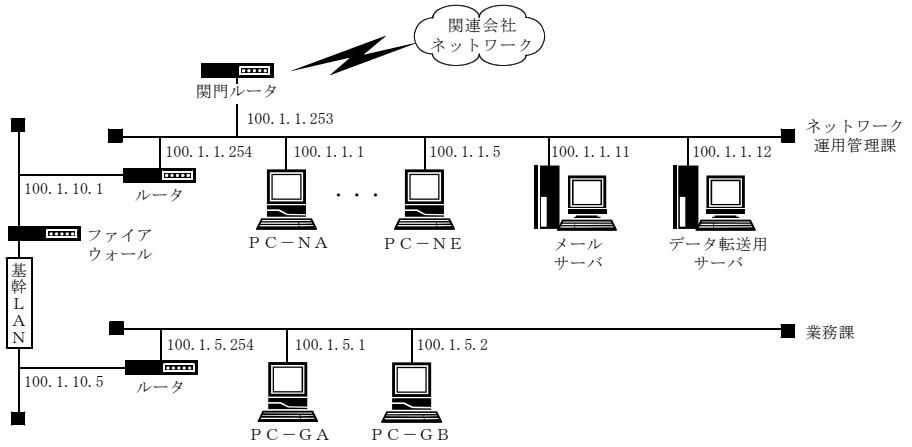


図　Ｘ社のＬＡＮ構成

関門ルータ内の設定テーブルの例を表１に示す。条件設定は，ＩＰ層での識別番号であるＩＰアドレスと，ＴＣＰ層での識別番号であるポート番号を組み合わせて行う。すなわち，設定テーブルの一つの行にＩＰアドレスとポート番号を指定すると，そのＩＰアドレス及びポート番号に該当するパケットだけが関門ルータを通過することができる。設定テーブルのＩＰアドレス欄に０．０．０．０又はポート番号欄に０を指定すると，その欄に関しては制限しないことを意味する。また，“：”を挟んで範囲を指定したときには，その範囲内のＩＰアドレス又はポート番号のパケットを通過させることを意味する。関門ルータを通過しようとするパケットの検査は，設定テーブルの最初の条件から順に行われ，どの条件にも適合しないパケットは破棄される。

表１　関門ルータ内の設定テーブルの例（ｔｅｌｎｅｔ対応）

	ＩＰ層		ＴＣＰ層	
	送信元ＩＰアドレス	あて先ＩＰアドレス	送信元ポート番号	あて先ポート番号
条件１	100.1.1.1：100.1.1.5	0.0.0.0	0	23
条件２	0.0.0.0	100.1.1.1：100.1.1.5	23	1026：65535

表１の設定例では，社内から社外への仮想端末機能（ｔｅｌｎｅｔ）サービスのパケット及びその返信である社外から社内へのｔｅｌｎｅｔサービスのパケットだけが通過できるように設定している。その結果，ネットワーク運用管理課のＰＣ－ＮＡ～ＰＣ－ＮＥ（ＩＰアドレスは１００．１．１．１～１００．１．１．５）からＸ社外のサーバが提供しているｔｅｌｎｅｔサービス（ポート番号は２３で固定）が利用できる。社外からのパケットは，ポート番号が１０２６以上のパケットだけを通すように設定している。

設問　Ｘ社の関連会社であるＹ社から，Ｘ社のＬＡＮに対する次の接続要請があった。

> Ｙ社の２台のパソコン（ＩＰアドレスは１０１．１．１．１と１０１．１．１．２）から，Ｘ社のネットワーク運用管理課のデータ転送用サーバ（ＩＰアドレスは１００．１．１．１２）へ接続して，データ転送機能サービスを利用したい。

この要請を満たすために，関門ルータの設定テーブルには，どのような条件を指定すればよいか。次の設定テーブルの［　　］に入れるべき値を解答群の中から選べ。ここで，データ転送にあたって，Ｘ社のサーバはポート番号１０２４と１０２５の二つを同時に利用するものとする。解答は，重複して選んでもよい。

表２　関門ルータ内の設定テーブル（データ転送対応）

ＩＰ層		ＴＣＰ層	
送信元ＩＰアドレス	あて先ＩＰアドレス	送信元ポート番号	あて先ポート番号
［a］	［b］	0	［c］
［b］	［a］	［d］	1026：65535

解答群

ア　0	イ　0.0.0.0	ウ　100.1.1.12
エ　100.1.1.12：101.1.1.1	オ　100.1.1.12：101.1.1.2	カ　101.1.1.1
キ　101.1.1.1：101.1.1.2	ク　1024	ケ　1024：1025
コ　1025		

a		b		c		d	

問４　パケットフィルタリングに関する次の記述を読んで，設問１，２に答えよ。

Ｘ社では，図に示すネットワークを構築し，インターネットへのＷｅｂサイトの公開と電子メール（以下，メールという）の送受信を行っている。

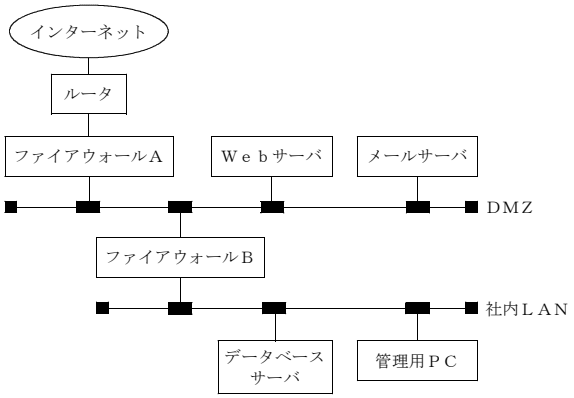


図　Ｘ社のネットワーク構成

Ｘ社のネットワークは二つのファイアウォールによって，ＤＭＺ及び社内ＬＡＮの二つのセグメントに分けられている。Ｗｅｂサーバ，メールサーバ及びデータベースサーバ（以下，ＤＢサーバという）は，それぞれ次の役割を果たしている。

(1) Ｗｅｂサーバ
　Ｗｅｂサイトとして，自社の情報をインターネットに公開する。Ｗｅｂサーバ上では，社外との取引情報を処理するプログラムが動作する。このプログラムが利用するデータはＤＢサーバ上に格納される。

(2) メールサーバ
　社外とのメールの送受信を行う。また，取引先に対してメールを自動配信するプログラムが動作する。メール配信のためのデータはＤＢサーバ上に格納される。

(3) ＤＢサーバ
　Ｗｅｂサーバ及びメールサーバで利用するデータを格納する。

社内ＬＡＮに接続された管理用ＰＣからは，ＳＳＨを使った各サーバへのログイン操作と，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から自社Ｗｅｂサーバの参照はできるが，社外Ｗｅｂサイトの利用は許可されていない。

ネットワーク上で使われるプロトコルとポート番号を表１に示す。

表１　プロトコルとポート番号

サービス	プロトコル	ポート番号
Ｗｅｂ	ＨＴＴＰ	８０
メール転送	ＳＭＴＰ	２５
セキュアシェル（遠隔ログイン）	ＳＳＨ	２２
メール受信	ＰＯＰ３	１１０
ＤＢアクセス	ＤＢ専用	１９９９

設問１　次の記述中の［　　］に入れる正しい答えを，解答群の中から選べ。解答は重複して選んでもよい。

　インターネットとＤＭＺをつなぐファイアウォールＡのパケットフィルタリングの設定を表２に示す。また，ＤＭＺと社内ＬＡＮをつなぐファイアウォールＢのパケットフィルタリングの設定を表３に示す。

　フィルタリングの設定ルールは，送信元のＩＰアドレス，あて先のＩＰアドレス及び接続先ポート番号を指定して通信の許可／拒否を制御する。設定は上の行のルールから調べて，最初に条件が合致した行の動作を実行する。また，応答パケットについては動的フィルタリング機能によって自動的に許可されるので設定は不要なものとする。

表２　ファイアウォールＡのフィルタリングの設定

条件			動作
送信元	あて先	ポート番号	
任意	Ｗｅｂサーバ	８０	許可
任意	メールサーバ	２５	許可
［ a ］	任意	［ b ］	許可
任意	任意	任意	拒否

表３　ファイアウォールＢのフィルタリングの設定

条件			動作
送信元	あて先	ポート番号	
Ｗｅｂサーバ	ＤＢサーバ	１９９９	許可
メールサーバ	ＤＢサーバ	１９９９	許可
管理用ＰＣ	［ c ］	［ d ］	許可
管理用ＰＣ	メールサーバ	２２	許可
管理用ＰＣ	メールサーバ	２５	許可
管理用ＰＣ	Ｗｅｂサーバ	８０	許可
管理用ＰＣ	Ｗｅｂサーバ	２２	許可
任意	任意	任意	拒否

a，ｃに関する解答群
　ア　ＤＢサーバ　　イ　Ｗｅｂサーバ　　ウ　管理用ＰＣ　　エ　メールサーバ　　オ　任意

b，ｄに関する解答群
　ア　２２　　イ　２５　　ウ　８０　　エ　１１０　　オ　１９９９

設問２　Ｘ社のネットワークでは，ファイアウォールによるパケットフィルタリングによって，インターネット接続に伴うセキュリティ上のリスクを低減しているが，パケットフィルタリングは，すべての脅威に対する防御とはならない。パケットフィルタリングによって防ぐことができるセキュリティ上のリスクとして，正しい答えを解答群の中から二つ選べ。

解答群
　ア　Ｗｅｂサイトとやり取りされるデータの盗聴や改ざん
　イ　Ｗｅｂサイトへの ＳＱＬインジェクション攻撃
　ウ　インターネットからＤＭＺ内のサーバへの許可されていないポートでの接続
　エ　インターネットから社内ＬＡＮへの不正アクセスによる攻撃
　オ　メールによる社内からのファイル流出

設問１	a		b		c		d		設問２		

問５　ネットワークシステムに関する次の記述を読んで，設問１～３に答えよ。

Ｘ社では，社外とのネットワーク接続にインターネットを利用している。社内の各部門ごとにＬＡＮがあり，複数のパソコンやサーバを接続する。パソコンやサーバには固定のプライベートＩＰアドレスを付与する。各部門のＬＡＮは，ルータを介して基幹ＬＡＮに接続する。インターネットへの接続は，基幹ＬＡＮ上の関門サーバが行う。関門サーバには，プロキシの機能，コンピュータウイルスを検出する機能，ファイアウォールの機能などが含まれている。

Ｘ社のネットワーク構成を，Ｙ部門とＺ部門を例にとって図に示す。図中の数字は，ＩＰアドレスを表す。

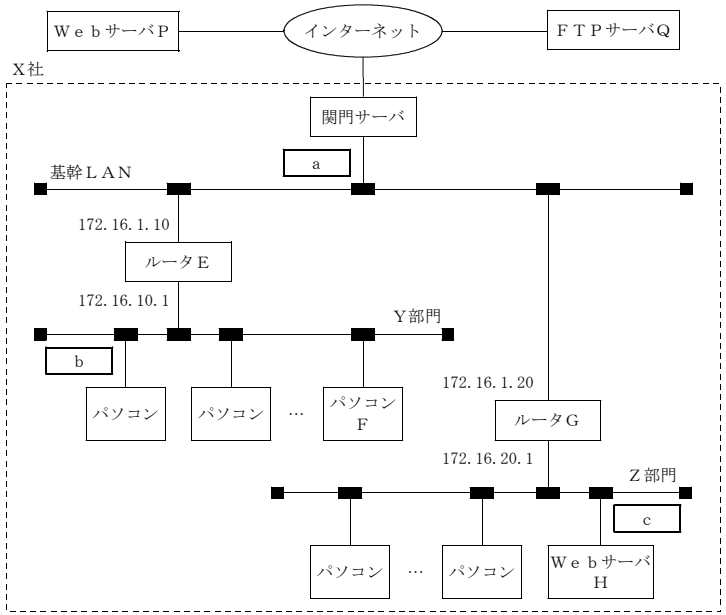


図　Ｘ社のネットワーク構成

設問１　図中の［　　］は，パソコンやサーバのＩＰアドレスを示す。指定可能なＩＰアドレスを，解答群の中から選べ。ここで，サブネットマスクは，255.255.255.0 とする。

解答群

ア	172.16.0.1	イ	172.16.0.2	ウ	172.16.1.1	エ	172.16.2.2
オ	172.16.10.1	カ	172.16.10.2	キ	172.16.10.255		
ク	172.16.20.1	ケ	172.16.20.2	コ	172.16.20.255		

設問２　次の表は，パソコンＦのブラウザからＺ部門のＷｅｂサーバＨにデータを送信する場合と，同じブラウザからインターネット上のＷｅｂサーバＰにデータを送信する場合の，データに付加するＩＰアドレスやＭＡＣアドレスがどのコンピュータのものであるかを示したものである。表中の［　　］に入れる正しい答えを，解答群の中から選べ。ただし，社内のＷｅｂサーバにアクセスする場合には，プロキシの機能を使用しないものとする。

表　データに付加するアドレス

送信先	パソコンＦが送信するデータ		送信先が受信するデータ
	送信先ＩＰアドレス	送信先ＭＡＣアドレス	送信元ＩＰアドレス
ＷｅｂサーバＨ	ＷｅｂサーバＨ		
ＷｅｂサーバＰ	ＷｅｂサーバＰ		

解答群

ア

ＷｅｂサーバＨ	パソコンＦ
ＷｅｂサーバＰ	関門サーバ

イ

ＷｅｂサーバＨ	パソコンＦ
ＷｅｂサーバＰ	パソコンＦ

ウ

ＷｅｂサーバＨ	パソコンＦ
関門サーバ	パソコンＦ

エ

ルータＥ	パソコンＦ
関門サーバ	パソコンＦ

オ

ルータＥ	パソコンＦ
ルータＥ	関門サーバ

設問３　次の記述中の［　　］に入れる正しい答えを，解答群の中から選べ。

パソコンＦからインターネット上のＦＴＰサーバＱにＦＴＰクライアントソフトで接続を試みたところ，うまく接続できなかった。しかし，パソコンＦで，ＦＴＰサーバＱを指定したｐｉｎｇコマンドを実行したところ，ＦＴＰサーバＱから応答があった。接続のための操作手順が正しいとすると，関門サーバの［　　］の設定に原因がある場合がある。

解答群

ア　Ｊａｖａアプレットの使用許可　　イ　クッキーの受入れ　　ウ　サブネットマスク
エ　通過可能なポート番号　　オ　ルーティングテーブル

設問１	a		b		c		設問２		設問３	

問６　利用者認証に関する次の記述を読んで，設問１，２に答えよ。

Ｘ社では，社外の端末から社内のサーバへのリモートログインを可能にするため，利用者認証の方式を検討している。社内では，利用者ＩＤとパスワードをサーバに送信する方式を使用しており，そのパスワードの強化を含め，次の三つの方式の安全性を検討している。

〔方式１：利用者ＩＤとパスワード方式〕

端末は，利用者が入力した利用者ＩＤとパスワードをサーバに送信する。サーバは利用者ＩＤから登録されているパスワードを検索し，送信されたパスワードと照合することによって，ログインの可否を応答する。利用者ＩＤとパスワード方式を図１に示す。

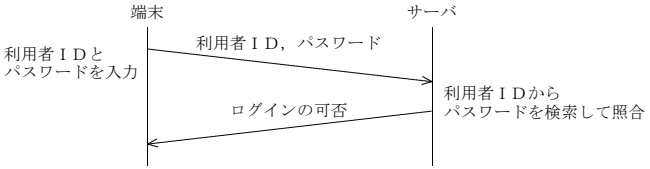


図１　利用者ＩＤとパスワード方式

〔方式２：チャレンジレスポンス方式〕

端末は，利用者が入力した利用者ＩＤをサーバに送信する。サーバは，利用者ＩＤを受信すると，ランダムに生成したチャレンジと呼ばれる値ｃを端末に送信する。端末は，利用者が入力したパスワードｐとチャレンジｃから，ハッシュ値ｈ(ｐ，ｃ)を計算して，レスポンスの値としてサーバに送信する。サーバは，利用者ＩＤから登録されているパスワードｐ’を検索し，端末と同じハッシュ関数ｈを使って計算したハッシュ値ｈ(ｐ’，ｃ)とレスポンスの値とを照合することによって，ログインの可否を応答する。ここで，ハッシュ関数ｈは公知のものであり，どの端末でも計算可能とする。チャレンジレスポンス方式を図２に示す。

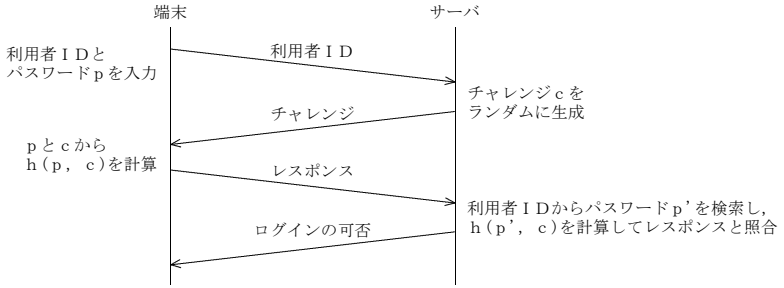


図２　チャレンジレスポンス方式

〔方式３：トークン（パスワード生成器）方式〕

利用者には，自身の利用者ＩＤが登録されたトークンと呼ばれるパスワード生成器を配布しておく。トークンの例を図３に示す。

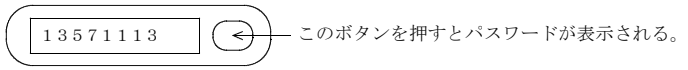


図３　トークンの例

トークンは時計を内蔵しており，関数ｇを使って，利用者ＩＤであるｕと時刻ｔに応じたパスワードｇ(ｕ，ｔ)を生成し表示することができる。利用者は，利用者ＩＤとトークンが生成し表示したパスワードを入力し，端末はこれらをサーバに送信する。サーバは，利用者ＩＤであるｕとサーバの時刻ｔからトークンと同じ関数ｇを使って生成したパスワードｇ(ｕ，ｔ)と端末から受信したパスワードとを照合することによって，ログインの可否を応答する。

なお，トークンの時刻とサーバの時刻が同期していることは保証されており，トークンのパスワード表示からサーバにおけるパスワード生成までの遅延も，一定の時間は許容する。トークン方式を図４に示す。

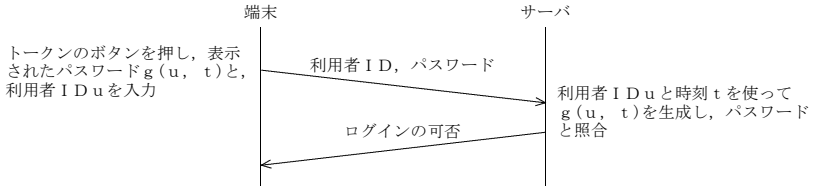


図４　トークン方式

設問１　パスワードの強度に関する次の記述中の［　　］に入れる正しい答えを，解答群の中から選べ。

方式１，２では，利用者がパスワードを設定する。これらの方式を採用する場合には，容易には推定されないパスワード，すなわち，十分な強度をもつパスワードを，利用者に設定してもらう必要がある。

パスワードの強度を高めるためには，パスワードを長くすることやパスワードに利用する文字の種類を増やすことが考えられる。例えば，英小文字２６文字だけからなる８文字のパスワードに対して，総当たり方式による発見に必要な最大時間を１とすると，パスワードの長さを１０文字にすれば必要な最大時間は［ a ］となる。また，同じ８文字であっても，英大文字も使用する場合，必要な最大時間は［ b ］となる。

解答群

ア　１.２５　　イ　２　　ウ　２０８　　エ　２５６　　オ　２６０
カ　６７６　　キ　１,０２４

設問２　盗聴のリスクに関する次の記述中の［　　］に入れる正しい答えを，解答群の中から選べ。解答は，重複して選んでもよい。

利用者認証の方式によっては，不正な方法によって入手した情報（例えば利用者ＩＤとパスワード）をそのまま利用することによって，不正ログインが行われる可能性がある。

(1) 社外からの通信経路上で通信内容が盗聴された場合，盗んだ情報をそのまま利用することによって，利用者がパスワードを変更しない限り，サーバへの不正ログインがいつでも可能になるのは，［ c ］である。ただし，通信経路は暗号化されていないものとする。

(2) 社外からのリモートログインに利用する端末上で，キーボード入力を読み取って，第三者に送信するプログラムが動作していた場合，盗んだ情報をそのまま利用することによって，利用者がパスワードを変更しない限り，サーバへの不正ログインがいつでも可能になるのは，［ d ］である。

(3) 誤って不正なサーバに接続して通常のログイン操作を行った場合，誤接続したサーバ上で端末から送信された情報が盗まれる場合がある。この盗んだ情報をそのまま利用することによって，利用者がパスワードを変更しない限り，サーバへの不正ログインがいつでも可能になるのは，［ e ］である。

解答群

ア　方式１だけ　　イ　方式２だけ　　ウ　方式３だけ
エ　方式１，２だけ　　オ　方式１，３だけ　　カ　方式２，３だけ
キ　方式１，２，３すべて

設問１	a		b		設問２	c		d		e	

問 7　認証システムに関する次の記述を読んで，設問に答えよ。

複数のクライアントと複数のアプリケーションサーバ（以下，ＡＰサーバという）が接続されているネットワークにおいて，単純な認証システムを利用する場合について，ここでは二つの問題点を取り上げる。

① 利用者は，使用するクライアントから各ＡＰサーバにログインするごとに，利用者ＩＤとパスワードの入力操作を行わなければならない。
② クライアントとＡＰサーバとの間の通信データの横取りと偽造によって，ＡＰサーバのサービスが不正に利用される危険性がある。

ここで，これらの問題を改善するための認証システム（以下，新認証システムという）を考える。
なお，ここでは，これらの問題に直接関連しない仕様については，その記述を省略する。

〔新認証システムによる問題点の解消〕
問題点①に対しては，利用者が一度，利用者ＩＤとパスワードをクライアントに入力して認証を受ければ，そのクライアントと各ＡＰサーバ間での認証は，利用者を介さないで済むように改善する。
このために，チケットと呼ぶ認証データを用いる。チケットは，クライアントに対して発行され，そのクライアントは，ＡＰサーバの認証を得るとき，発行されたチケットをＡＰサーバに送信する。
問題点②に対しては，ＡＰサーバに送信されたチケットが，チケットの発行を受けたクライアントから送られてきたものであることを，ＡＰサーバが確認できるよう，チケットとは別に認証子と呼ぶ認証データを用いる。

図１に新認証システムの構成を示す。

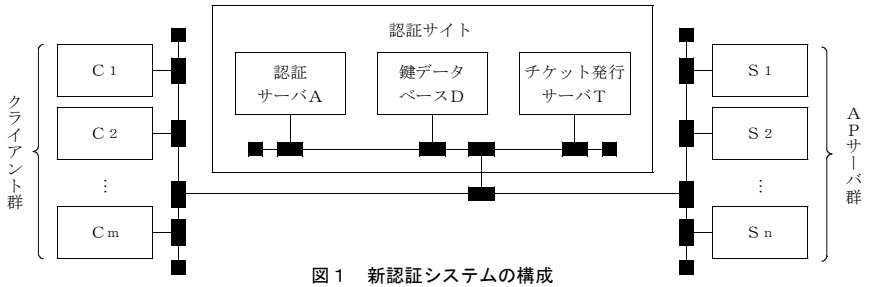
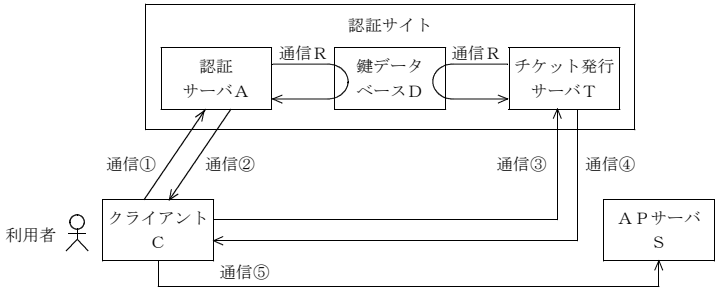


図１　新認証システムの構成

〔新認証システムの構成と方式についての説明〕
(1) 新認証システムでは，共通鍵暗号方式によって，通信データを暗号化する。以下，共通鍵を鍵という。
(2) 認証サイトは，認証サーバ，鍵データベース及びチケット発行サーバで構成する。
(3) チケット発行サーバの鍵は，チケット発行サーバ自体と鍵データベースに登録されている。
(4) 各ＡＰサーバの鍵は，それぞれのＡＰサーバ自体と鍵データベースに登録されている。
(5) 利用者の鍵は，利用者のパスワードから計算して決められ，鍵データベースに登録されている。クライアントには，利用者が入力したパスワードから計算した鍵が，利用者がクライアントの利用を終了するまで，一時的に保持される。

〔認証のための通信の例〕
図２は，利用者が，クライアントＣから目的のＡＰサーバＳにアクセスする場合の認証の流れを示す。



注　通信Ｒは，鍵データベースを参照していることを表す。

図２　認証の流れの例

認証は，次の３段階で行われる。ここで，ｅｎｃ(ｘ)は，ｘを暗号化したものを表す。

第１段階は，クライアントＣがチケット発行サーバＴにチケットを要求するためのチケット（以下，チケット発行サーバＴ用チケットという）の認証サーバＡへの要求（図２中の通信①）と，その発行（図２中の通信②）である。
通信①では，クライアントＣは，次のデータを認証サーバＡに送信する。

データ	データの説明
ID_C	利用者ＩＤである。
ID_T	チケット発行サーバＴのＩＤである。

通信②では，認証サーバＡは，次のデータをクライアントＣに応答する。

データ	データの暗号化に用いた鍵	データの説明
$enc(KEY_{CT})$	利用者の鍵 KEY_C	KEY_{CT}は，クライアントＣとチケット発行サーバＴとの間（以下，Ｃ－Ｔ間という）の通信データの暗号化に用いる鍵であり，Ｃ－Ｔ間のセッション鍵という。
$enc(TICKET_{CT})$	a	$TICKET_{CT}$は，チケット発行サーバＴ用チケットである。$TICKET_{CT}$はKEY_{CT}を含む。これによって，チケット発行サーバＴにクライアントＣ経由でKEY_{CT}を安全に渡すことができる。

第２段階は，クライアントＣがＡＰサーバＳにアクセスするためのチケット（以下，ＡＰサーバＳ用チケットという）のチケット発行サーバＴへの要求（図２中の通信③）と，その発行（図２中の通信④）である。
通信③では，クライアントＣは，次のデータをチケット発行サーバＴに送信する。

データ	データの暗号化に用いた鍵	データの説明
$enc(TICKET_{CT})$	a	$enc(TICKET_{CT})$は，クライアントＣでは復号できない。クライアントＣは，チケット発行サーバＴにそのまま送信し，チケット発行サーバＴが復号する。
$enc(AUTH_{C1})$	b	認証子$AUTH_{C1}$は，クライアントＣが生成する。
$enc(ID_S)$	b	認証子ID_Sは，ＡＰサーバＳのＩＤである。

チケット発行サーバTは，ＴＩＣＫＥＴ$_{CT}$を送信したのが間違いなくクライアントＣであることをＴＩＣＫＥＴ$_{CT}$とＡＵＴＨ$_{C1}$から確認する。確認ができたとき，通信④では，チケット発行サーバTは，次のデータをクライアントＣに応答する。

データ	データの暗号化に用いた鍵	データの説明
ｅｎｃ(ＫＥＹ$_{CS}$)	b	ＫＥＹ$_{CS}$は，クライアントＣとＡＰサーバＳとの間（以下，Ｃ－Ｓ間という）の通信データの暗号化に用いる鍵であり，Ｃ－Ｓ間のセッション鍵という。データの暗号化に用いた鍵は，チケット発行サーバTが，通信③で受け取ったｅｎｃ(ＴＩＣＫＥＴ$_{CT}$)から取り出したものである。
ｅｎｃ(ＴＩＣＫＥＴ$_{CS}$)	c	ＴＩＣＫＥＴ$_{CS}$は，ＡＰサーバＳ用チケットである。ＴＩＣＫＥＴ$_{CS}$はＫＥＹ$_{CS}$を含む。これによって，ＡＰサーバＳにＫＥＹ$_{CS}$をクライアントＣ経由で安全に渡すことができる。

第３段階は，ＡＰサーバＳ用チケットの提示である（図２中の通信⑤）。
通信⑤では，クライアントＣは，次のデータをＡＰサーバＳに送信する。

データ	データの暗号化に用いた鍵	データの説明
ｅｎｃ(ＴＩＣＫＥＴ$_{CS}$)	c	ｅｎｃ(ＴＩＣＫＥＴ$_{CS}$)は，クライアントＣでは復号できない。クライアントＣは，ＡＰサーバＳにそのまま送信し，ＡＰサーバＳが復号する。
ｅｎｃ(ＡＵＴＨ$_{C2}$)	d	認証子ＡＵＴＨ$_{C2}$は，クライアントＣが生成する。

ＡＰサーバＳは，ＴＩＣＫＥＴ$_{CS}$を送信したのが間違いなくクライアントＣであることをＴＩＣＫＥＴ$_{CS}$とＡＵＴＨ$_{C2}$から確認する。確認ができたとき，利用者は，クライアントＣから，ＡＰサーバＳへのアクセスが許可される。

設問　本文中の［　　］に入れる正しい答えを，解答群の中から選べ。

aに関する解答群
ア　Ｃ－Ｔ間のセッション鍵ＫＥＹ$_{CT}$　　イ　チケット発行サーバTのＩＤ　ＩＤ$_{T}$
ウ　チケット発行サーバTの鍵ＫＥＹ$_{T}$　　エ　利用者ＩＤ　ＩＤ$_{C}$

b，cに関する解答群
ア　ＡＰサーバＳのＩＤ　ＩＤ$_{S}$　　イ　ＡＰサーバＳの鍵ＫＥＹ$_{S}$
ウ　Ｃ－Ｓ間のセッション鍵ＫＥＹ$_{CS}$　　エ　Ｃ－Ｔ間のセッション鍵ＫＥＹ$_{CT}$
オ　チケット発行サーバTの鍵ＫＥＹ$_{T}$

dに関する解答群
ア　ＡＰサーバＳの鍵ＫＥＹ$_{S}$　　イ　Ｃ－Ｓ間のセッション鍵ＫＥＹ$_{CS}$
ウ　Ｃ－Ｔ間のセッション鍵ＫＥＹ$_{CT}$　　エ　チケット発行サーバTの鍵ＫＥＹ$_{T}$

a		b		c		d	