問３　ネットワークの構築（ネットワーク）　(H23 秋-FE 午後問 3)

【解答】

［設問１］　a－ウ，b－イ

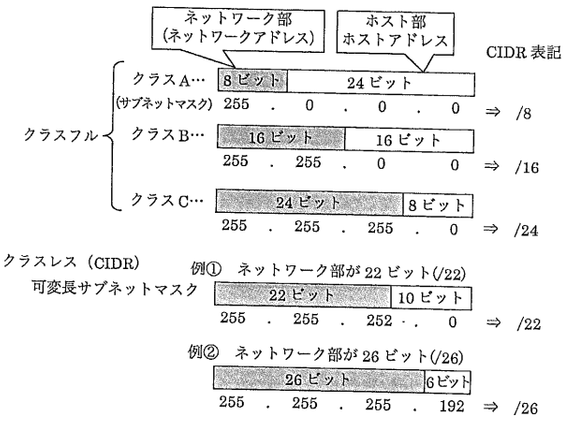
［設問２］　c－エ，d－ア，e－カ

【解説】

IP ネットワークの構築に関する基本的な問題である。設問 1 は，IP アドレスの構成やサブネットマスクなどの知識があれば解答できる。設問 2 は DHCP とブロードキャストに関する知識や，プロキシサーバの知識が必要である。いずれも，基本的な知識で解答できる問題であるが，キャッシュサーバの問題は，キャッシュメモリに関する知識の応用が必要である。

まずは，IP アドレス（IPv4 アドレス）の基本的な構成について解説する。

図 A に示すように，32 ビットの IP アドレス（IPv4 アドレス）は，ネットワーク部（ネットワークアドレス）とホスト部（ホストアドレス）から構成されている。ネットワーク部は，インターネット上に存在する各組織のネットワークを一意に識別する情報である。また，ホスト部は，各々のネットワークの上のホストを一意に識別する情報である。ここで言うホストは，汎用の大型コンピュータではなく，サーバやパソコン，更にルータなどの IP ネットワーク機器全般を示す。要は，IP を使用して通信を行うすべてのシステムがホストであり，各ホストには IP アドレスなどを設定する必要がある。



図A　IP アドレスの構成とサブネットマスク

IP アドレスには，クラスと呼ぶ概念があり，クラス A～クラス C が一般的に知られている。このクラスによるネットワークの分類方法をクラスフルと呼ぶ。各クラスは，ネットワーク部の長さが異なり，クラス A のネットワーク部の長さは 8 ビット，クラス B のネットワーク部の長さは 16 ビット，クラス C のネットワーク部の長さは 24 ビットである。ホスト部の長さは，全体の 32 ビットから各クラスのネットワーク部の長さを引き算したものとなる。よって，クラス A のホスト部の長さは 24 ビット，クラス B は 16 ビット，クラス C は 8 ビットとなる。このホスト部の長さは，ネットワークに接続できるホストの最大台数を決める。クラス A では 2^{24}(16777216)，クラス B では 2^{16}(65536)，クラス C では 2^{8}(256)となるが，ホストに割り付けできないアドレスが 2 個あるため，接続できるホスト台数は 2 を引いた値となる。よって，最大台数は，クラス A では 16,777,214 台，クラス B では 65,534 台，クラス C では 254 台となる。

また，ネットワーク部とホスト部を識別する情報が必要である。これが，サブネットマスクである。サブネットマスクは IP アドレスと同じ 32 ビットで，ネットワーク部をビットの 1 で示す。サブネットマスクの表記は IP と同様に 8 ビットごとに区切り，10 進数で表す。クラス A の場合は 255.0.0.0，クラス B の場合は 255. 255.0.0，クラス C の場合は 255. 255. 255.0 となる。（図 A のサブネットマスクを参照）IP アドレスとサブネットマスクの論理積（AND）を取ることによって，ネットワークアドレスを抽出することができる。

しかし，クラスフルの概念では，ネットワーク部の長さが決まっており，利用しづらいことがある。例えば，クラス A の最大ホスト台数は 16,777,214 台であるが，16,777,214 台のホストを一つのネットワークに接続することは，実際にはあり得ないことであり，使用していない無駄なアドレスが大量に存在することになる。逆にクラス C の 254 台ではアドレスが足りないこともあり得る。

そこで，現在ではクラスの概念を排して，ネットワーク部を任意の長さに設定することができる。これを CIDR（Classless Inter-Domain Routing（サイダー））と呼ぶ。最近ではこのクラスレスの考え方を用いることが多い。図 A の例①では，ネットワーク部が 22 ビット，ホスト部が 10 ビットの例である。この場合，ネットワークに接続できるホスト台数は 2^{10}（1024）から 2 を引いた，1,022 台となる。例②では，ネットワーク部が 26 ビット，ホスト部が 6 ビットの例である。この場合，ネットワークに接続できるホスト台数は 2^{6}(64)から 2 を引いた，62 台となる。

また，サブネットマスクの表現として，/（スラッシュ）とサブネットマスクの先頭から 1 のビットの数を用いて表現する CIDR 表記を使うことも多い。CIDR 表記では，クラス A 相当の 255.0.0.0 のサブネットマスクの場合，/8 となる。（図 A の右端を参照）

［設問１］

・空欄 a：問題の図 1 の D 社の現在のネットワーク構成には，DMZ，基幹ネットワーク，ネットワーク A，ネットワーク B が存在する。DMZ（DeMilitarized Zone）は直訳すると非武装地帯であるが，バリアセグメントと呼ぶ場合もある。DMZ は，社内ネットワーク（ここでは基幹ネットワーク）とインターネット側の間に設置するネットワークである。一般的にはファイアウォールで，インターネットと DMZ 間の通信と，DMZ と社内ネットワーク間の通信だけを許可することによって，インターネットと社内ネットワーク間の直接通信を遮断する設定を行う。これによって，インターネット側から社内ネットワークへの直接アクセスが不可能となり，外部からの直接攻撃のリスクを下げることができる。

なお，ファイアウォールは，IP パケットを転送するので，一種のルータでもある。ちなみに最近のルータはパケットフィルタリングなどのファイアウォール機能を持つことがほとんどである。

ルータは異なる IP ネットワーク間で IP パケットの経路を決め転送する（IP ルーティング）ための，機器である。言い換えると，異なる IP ネットワーク間のゲートウェイ（出入り口）である。そのため，ルータのインタフェース（ポート）に接続するネットワークは，各々異なる IP ネットワークであり，異なるネットワークアドレス部を持つ。

問題の図 1 において，各ルータのインタフェース（ポート）に記載された IP アドレスに注目すると，基幹ネットワークは 10.0.0.2 と 10.0.0.3 である。また，ネットワーク A は 10.0.1.1 と 10.0.1.200，ネットワーク B は 10.0.2.1 である。これを表 A に整理する。

表A　D 社のネットワーク

各ネットワーク内でホストを一意に識別できる

ネットワーク	IP アドレス（10 進数）	IP アドレス（2 進数）
基幹ネットワーク	10.0.0.2	0000 1010 .0000 0000 .0000 0000 .0000 0010
	10.0.0.3	0000 1010 .0000 0000 .0000 0000 .0000 0011
ネットワークA	10.0.1.1	0000 1010 .0000 0000 .0000 0001 .0000 0001
	10.0.1.200	0000 1010 .0000 0000 .0000 0001 .1100 1000
ネットワークB	10.0.2.1	0000 1010 .0000 0000 .0000 0010 .0000 0001
サブネットマスク	255.255.255.0	ネットワーク部がこの範囲だと，ネットワークを一意に識別できる 1111 1111 .1111 1111 .1111 1111 .0000 0000 ネットワーク部のビットは 1（先頭から 24 個 1 が並ぶ）　ホスト部のビットは 0

ここで，基幹ネットワークに注目すると，10.0.0.まで同じであり，それ以降のアドレスは変化している。また，ネットワーク A に注目すると，10.0.1.まで同じであり，以降のアドレスは変化している。このことによって，表 A に示すネットワークアドレスの下線部※が，ネットワークを識別するためのネットワーク部，それ以降がホスト部と推測できる。

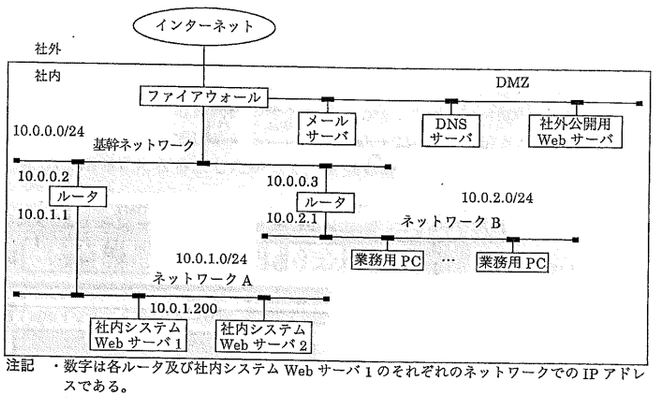
（※ネットワーク部を示す下線は，解説用の便宜上のものであり，通常は書かない。）

ここで念の為，各ネットワークアドレスを 2 進数に変換して考えてみる。すると，ネットワークごとに，ネットワークを一意に識別できるのは，矢印の範囲（先頭ビットから 24 ビットまで）であることが分かる。ネットワーク A には 10.0.1.1 と 10.0.1.200 の二つのホストがあるが，ネットワーク部が矢印の範囲であれば，二つのホスト部を一意に識別できる。また，基幹ネットワークも 10.0.0.2 と 10.0.0.3 であるので，二つのホスト部を一意に識別できる。

よって，サブネットマスクは先頭ビットから 24 ビット目までで（/24）あり，10 進数のサブネットマスクの表記では，255. 255. 255.0 となる。

したがって，空欄 a は（ウ）が正解となる。

なお，図 B に各ネットワークの範囲とネットワークアドレスを記載した図を示しておく。



注記　・数字は各ルータ及び社内システム Web サーバ 1 のそれぞれのネットワークでの IP アドレスである。
・網掛け部分は，各ネットワークの範囲を示す。

図B　ネットワークの IP アドレス

・空欄 b：次にネットワーク A に割り当て可能な IP アドレスを考える。前述のようにサブネットマスクは 255. 255. 255.0 であるから，ネットワーク A のネットワーク部（ネットワークアドレス）は，10.0.1.0 となる。よって，〔IP アドレス〕の選択肢のうち，ネットワーク部が 10.0.1.0 に一致するのは，10.0.1.1，10.0.1.2，10.0.1.3 の 3 個である。しかし，10.0.1.1 は既に使用されているため，設定可能なものは 2 個になる。したがって，空欄 b は（イ）が正解となる。なお，参考までに問題の IP アドレス（10.0.0.～，10.0.1.～10.0.2.～）は LAN の内部で利用するプライベート IP アドレス（クラス用）である。

［設問２］

・空欄 c：DHCP（Dynamic Host Configuration Protocol）は，IP アドレスと関連する情報を自動的に割り振り，IP アドレスやサブネットマスクなどの IP 通信に不可欠な情報を自動設定するためのプロトコルである。クライアントに割付け可能な IP アドレスを管理し，IP アドレスを払い出すサーバを DHCP サーバと呼び，IP アドレスを DHCP サーバから割り当ててもらうホストを DHCP クライアントと呼ぶ。DHCP クライアントは固定の IP アドレスを持たない。そのため，DHCP クライアントが起動すると，DHCP サーバを探して IP アドレスの候補を通知してもらうために DHCP DISCOVER と呼ぶメッセージをブロードキャストで送信する。ブロードキャストは同一ネットワーク上に存在するすべてのホスト機器への一斉送信である。ブロードキャストで送信したパケットは，ルータを超えることはできない。（もし，ブロードキャストのパケット

問３　ネットワークの構築（ネットワーク）　(H23 秋-FE 午後問 3)

【解答】

［設問１］　a－ウ，b－イ

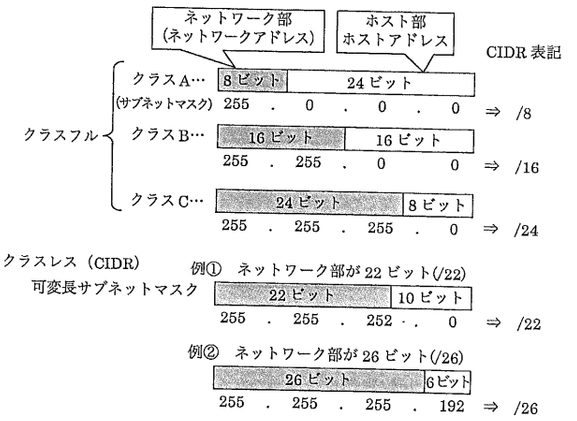
［設問２］　c－エ，d－ア，e－カ

【解説】

IP ネットワークの構築に関する基本的な問題である。設問 1 は，IP アドレスの構成やサブネットマスクなどの知識があれば解答できる。設問 2 は DHCP とブロードキャストに関する知識や，プロキシサーバの知識が必要である。いずれも，基本的な知識で解答できる問題であるが，キャッシュサーバの問題は，キャッシュメモリに関する知識の応用が必要である。

まずは，IP アドレス（IPv4 アドレス）の基本的な構成について解説する。

図 A に示すように，32 ビットの IP アドレス（IPv4 アドレス）は，ネットワーク部（ネットワークアドレス）とホスト部（ホストアドレス）から構成されている。ネットワーク部は，インターネット上に存在する各組織のネットワークを一意に識別する情報である。また，ホスト部は，各々のネットワークの上のホストを一意に識別する情報である。ここで言うホストは，汎用の大型コンピュータではなく，サーバやパソコン，更にルータなどの IP ネットワーク機器全般を示す。要は，IP を使用して通信を行うすべてのシステムがホストであり，各ホストには IP アドレスなどを設定する必要がある。



図A　IP アドレスの構成とサブネットマスク

IP アドレスには，クラスと呼ぶ概念があり，クラス A～クラス C が一般的に知られている。このクラスによるネットワークの分類方法をクラスフルと呼ぶ。各クラスは，ネットワーク部の長さが異なり，クラス A のネットワーク部の長さは 8 ビット，クラス B のネットワーク部の長さは 16 ビット，クラス C のネットワーク部の長さは 24 ビットである。ホスト部の長さは，全体の 32 ビットから各クラスのネットワーク部の長さを引き算したものとなる。よって，クラス A のホスト部の長さは 24 ビット，クラス B は 16 ビット，クラス C は 8 ビットとなる。このホスト部の長さは，ネットワークに接続できるホストの最大台数を決める。クラス A では 2^{24}(16777216)，クラス B では 2^{16}(65536)，クラス C では 2^{8}(256)となるが，ホストに割り付けできないアドレスが 2 個あるため，接続できるホスト台数は 2 を引いた値となる。よって，最大台数は，クラス A では 16,777,214 台，クラス B では 65,534 台，クラス C では 254 台となる。

また，ネットワーク部とホスト部を識別する情報が必要である。これが，サブネットマスクである。サブネットマスクは IP アドレスと同じ 32 ビットで，ネットワーク部をビットの 1 で示す。サブネットマスクの表記は IP と同様に 8 ビットごとに区切り，10 進数で表す。クラス A の場合は 255.0.0.0，クラス B の場合は 255. 255.0.0，クラス C の場合は 255. 255. 255.0 となる。（図 A のサブネットマスクを参照）IP アドレスとサブネットマスクの論理積（AND）を取ることによって，ネットワークアドレスを抽出することができる。

しかし，クラスフルの概念では，ネットワーク部の長さが決まっており，利用しづらいことがある。例えば，クラス A の最大ホスト台数は 16,777,214 台であるが，16,777,214 台のホストを一つのネットワークに接続することは，実際にはあり得ないことであり，使用していない無駄なアドレスが大量に存在することになる。逆にクラス C の 254 台ではアドレスが足りないこともあり得る。

そこで，現在ではクラスの概念を排して，ネットワーク部を任意の長さに設定することができる。これを CIDR（Classless Inter-Domain Routing（サイダー））と呼ぶ。最近ではこのクラスレスの考え方を用いることが多い。図 A の例①では，ネットワーク部が 22 ビット，ホスト部が 10 ビットの例である。この場合，ネットワークに接続できるホスト台数は 2^{10}（1024）から 2 を引いた，1,022 台となる。例②では，ネットワーク部が 26 ビット，ホスト部が 6 ビットの例である。この場合，ネットワークに接続できるホスト台数は 2^{6}(64)から 2 を引いた，62 台となる。

また，サブネットマスクの表現として，/（スラッシュ）とサブネットマスクの先頭から 1 のビットの数を用いて表現する CIDR 表記を使うことも多い。CIDR 表記では，クラス A 相当の 255.0.0.0 のサブネットマスクの場合，/8 となる。（図 A の右端を参照）

［設問１］

・空欄 a：問題の図 1 の D 社の現在のネットワーク構成には，DMZ，基幹ネットワーク，ネットワーク A，ネットワーク B が存在する。DMZ（DeMilitarized Zone）は直訳すると非武装地帯であるが，バリアセグメントと呼ぶ場合もある。DMZ は，社内ネットワーク（ここでは基幹ネットワーク）とインターネット側の間に設置するネットワークである。一般的にはファイアウォールで，インターネットと DMZ 間の通信と，DMZ と社内ネットワーク間の通信だけを許可することによって，インターネットと社内ネットワーク間の直接通信を遮断する設定を行う。これによって，インターネット側から社内ネットワークへの直接アクセスが不可能となり，外部からの直接攻撃のリスクを下げることができる。

なお，ファイアウォールは，IP パケットを転送するので，一種のルータでもある。ちなみに最近のルータはパケットフィルタリングなどのファイアウォール機能を持つことがほとんどである。

ルータは異なる IP ネットワーク間で IP パケットの経路を決め転送する（IP ルーティング）ための，機器である。言い換えると，異なる IP ネットワーク間のゲートウェイ（出入り口）である。そのため，ルータのインタフェース（ポート）に接続するネットワークは，各々異なる IP ネットワークであり，異なるネットワークアドレス部を持つ。

問題の図 1 において，各ルータのインタフェース（ポート）に記載された IP アドレスに注目すると，基幹ネットワークは 10.0.0.2 と 10.0.0.3 である。また，ネットワーク A は 10.0.1.1 と 10.0.1.200，ネットワーク B は 10.0.2.1 である。これを表 A に整理する。

表A　D 社のネットワーク

各ネットワーク内でホストを一意に識別できる

ネットワーク	IP アドレス（10 進数）	IP アドレス（2 進数）
基幹ネットワーク	10.0.0.2	0000 1010 .0000 0000 .0000 0000 .0000 0010
	10.0.0.3	0000 1010 .0000 0000 .0000 0000 .0000 0011
ネットワークA	10.0.1.1	0000 1010 .0000 0000 .0000 0001 .0000 0001
	10.0.1.200	0000 1010 .0000 0000 .0000 0001 .1100 1000
ネットワークB	10.0.2.1	0000 1010 .0000 0000 .0000 0010 .0000 0001
サブネットマスク	255.255.255.0	ネットワーク部がこの範囲だと，ネットワークを一意に識別できる 1111 1111 .1111 1111 .1111 1111 .0000 0000 ネットワーク部のビットは 1（先頭から 24 個 1 が並ぶ）　ホスト部のビットは 0

ここで，基幹ネットワークに注目すると，10.0.0.まで同じであり，それ以降のアドレスは変化している。また，ネットワーク A に注目すると，10.0.1.まで同じであり，以降のアドレスは変化している。このことによって，表 A に示すネットワークアドレスの下線部※が，ネットワークを識別するためのネットワーク部，それ以降がホスト部と推測できる。

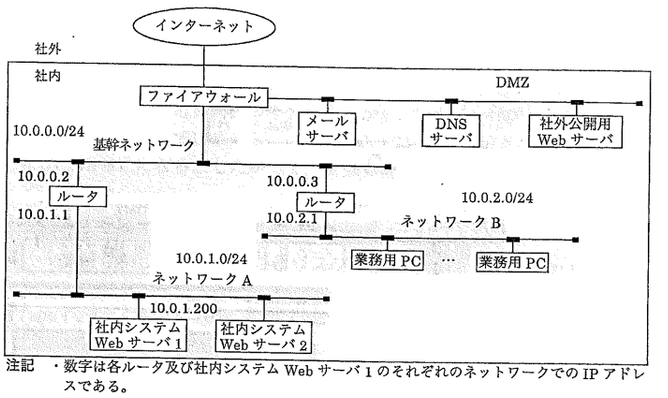
（※ネットワーク部を示す下線は，解説用の便宜上のものであり，通常は書かない。）

ここで念の為，各ネットワークアドレスを 2 進数に変換して考えてみる。すると，ネットワークごとに，ネットワークを一意に識別できるのは，矢印の範囲（先頭ビットから 24 ビットまで）であることが分かる。ネットワーク A には 10.0.1.1 と 10.0.1.200 の二つのホストがあるが，ネットワーク部が矢印の範囲であれば，二つのホスト部を一意に識別できる。また，基幹ネットワークも 10.0.0.2 と 10.0.0.3 であるので，二つのホスト部を一意に識別できる。

よって，サブネットマスクは先頭ビットから 24 ビット目までで（/24）あり，10 進数のサブネットマスクの表記では，255. 255. 255.0 となる。

したがって，空欄 a は（ウ）が正解となる。

なお，図 B に各ネットワークの範囲とネットワークアドレスを記載した図を示しておく。



注記　・数字は各ルータ及び社内システム Web サーバ 1 のそれぞれのネットワークでの IP アドレスである。
・網掛け部分は，各ネットワークの範囲を示す。

図B　ネットワークの IP アドレス

・空欄 b：次にネットワーク A に割り当て可能な IP アドレスを考える。前述のようにサブネットマスクは 255. 255. 255.0 であるから，ネットワーク A のネットワーク部（ネットワークアドレス）は，10.0.1.0 となる。よって，〔IP アドレス〕の選択肢のうち，ネットワーク部が 10.0.1.0 に一致するのは，10.0.1.1，10.0.1.2，10.0.1.3 の 3 個である。しかし，10.0.1.1 は既に使用されているため，設定可能なものは 2 個になる。したがって，空欄 b は（イ）が正解となる。なお，参考までに問題の IP アドレス（10.0.0.～，10.0.1.～10.0.2.～）は LAN の内部で利用するプライベート IP アドレス（クラス用）である。

［設問２］

・空欄 c：DHCP（Dynamic Host Configuration Protocol）は，IP アドレスと関連する情報を自動的に割り振り，IP アドレスやサブネットマスクなどの IP 通信に不可欠な情報を自動設定するためのプロトコルである。クライアントに割付け可能な IP アドレスを管理し，IP アドレスを払い出すサーバを DHCP サーバと呼び，IP アドレスを DHCP サーバから割り当ててもらうホストを DHCP クライアントと呼ぶ。DHCP クライアントは固定の IP アドレスを持たない。そのため，DHCP クライアントが起動すると，DHCP サーバを探して IP アドレスの候補を通知してもらうために DHCP DISCOVER と呼ぶメッセージをブロードキャストで送信する。ブロードキャストは同一ネットワーク上に存在するすべてのホスト機器への一斉送信である。ブロードキャストで送信したパケットは，ルータを超えることはできない。（もし，ブロードキャストのパケット