NW

令和７年度　春期
ネットワークスペシャリスト試験
午後Ⅰ　問題

試験時間	12:30 ～ 14:00（1 時間 30 分）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. 答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。
4. 問題は，次の表に従って解答してください。

問題番号	問１～問３
選択方法	２問選択

5. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) B 又は HB の黒鉛筆又はシャープペンシルを使用してください。
   (2) 受験番号欄に受験番号を，生年月日欄に受験票の生年月日を記入してください。正しく記入されていない場合は，採点されないことがあります。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入してください。
   (3) 選択した問題については，次の例に従って，選択欄の問題番号を○印で囲んでください。○印がない場合は，採点されません。3 問とも○印で囲んだ場合は，はじめの 2 問について採点します。
   (4) 解答は，問題番号ごとに指定された枠内に記入してください。
   (5) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

〔問１，問３を選択した場合の例〕

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

問１　ルータの更改に関する次の記述を読んで，設問に答えよ。

A 社は，従業員 800 人の建設機械販売会社である。大阪本社のほか，東京に支社を構えている。大阪本社と東京支社間は，広域イーサネットサービス網と IPsec VPN の冗長構成（以下，WAN という）で接続されている。A 社のネットワーク（以下，A 社 NW という）はインターネットと接続している。また，WAN を経由してプライベートクラウドである C 社の SaaS（以下，C 社 SaaS という）と接続している。

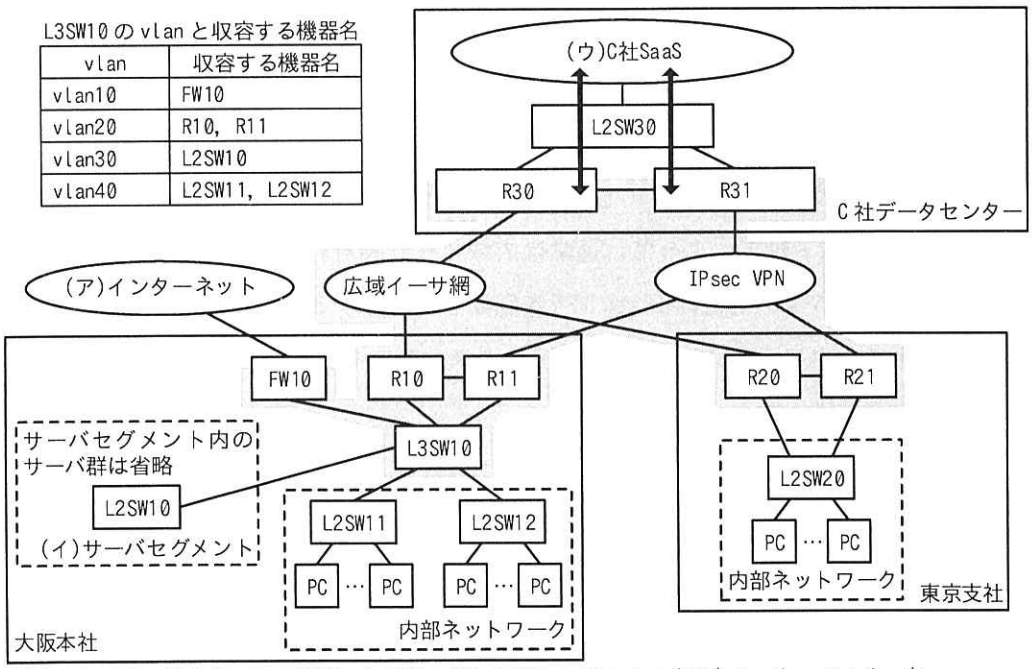
A 社 NW の一部を構成するルータのメーカーサポートが終了するので，A 社情報システム部はルータの更改プロジェクトを立ち上げ，ネットワーク担当の B さんが担当することになった。

〔現在の A 社 NW〕

現在の A 社 NW を図 1 に示す。

L3SW10 の vlan と収容する機器名

vlan	収容する機器名
vlan10	FW10
vlan20	R10，R11
vlan30	L2SW10
vlan40	L2SW11，L2SW12



L2SW：レイヤー２スイッチ　L3SW：レイヤー３スイッチ　FW：ファイアウォール　R：ルータ
広域イーサ網：広域イーサネットサービス網　　：OSPF のエリアの範囲　⟷：eBGP のピア

注記 1　FW10 と L3SW10 は冗長構成であるが，図では省略している。
注記 2　L3SW10 のポートは全てアクセスポートである。

図 1　現在の A 社 NW（抜粋）

現在の A 社 NW の概要を次に示す。

・A 社の従業員は，内部ネットワークの PC を利用して，インターネットやサーバセグメント内のサーバ群及び C 社 SaaS と通信し，業務を行っている。
・A 社 NW では，動的経路制御の一つである OSPF を利用している。
・IPsec VPN は DMVPN (Dynamic Multipoint VPN) を用いて広域イーサ網と同様のフルメッシュトポロジを実現している。また，IPsec VPN は，次に示すように広域イーサ網と同様の経路制御を行っている。
・A 社 NW の OSPF のエリアは，エリア ID が 0.0.0.0 と表記される，［ a ］エリアだけで構成されている。
・FW10，R10，R11，L3SW10，R20，R21，R30，R31 の各機器が OSPF ルータとして動作している。
・OSPF ルータにはループバックインタフェースが作成され，ループバック IP アドレスが設定されている。ループバック IP アドレスは，OSPF ルータを識別する［ b ］ID として利用されている。
・OSPF の経路交換をしないインタフェースは，パッシブインタフェースとして設定されている。
・OSPF の経路交換をするインタフェースでは，① OSPF のネイバー認証を行うことで，安全に経路交換をするようにしている。
・OSPF のコスト設定によって，通常は広域イーサ網を利用して通信し，広域イーサ網で通信できない場合は IPsec VPN を利用して通信する設計にしている。OSPF ルータの各インタフェースにおける OSPF のコスト設定を表 1 に示す。

表 1　OSPF ルータの各インタフェースにおける OSPF コスト設定

項番	OSPF ルータのインタフェース種別	OSPF コスト設定
1	広域イーサ網接続インタフェース	100
2	IPsec VPN 接続インタフェース	1000
3	ループバックインタフェース	1
4	その他のインタフェース	10

・FW10 は，インターネットに向けたデフォルトルートを設定しており，OSPF にインターネット向けのデフォルトルートの配布を行っている。
・FW10 はインターネットと接続し，NAPT によって IP アドレスとポート番号の変換を

行っている。

・R30，R31 と C 社 SaaS は eBGP で接続し，経路交換を行っている。eBGP 接続は認証を行うことで，安全に経路交換をするようにしている。

・② R30，R31 は，eBGP で経路広告する際に AS_PATH プリペンド設定をしている。通常は R30 を利用して通信し，R30 を利用して通信できない場合は R31 を利用して通信する設計にしている。

・R30，R31 は，eBGP の経路を OSPF に再配布を行っている。

・R30，R31 は，OSPF の経路を eBGP に再配布し，経路広告している。

・R30，R31 は，eBGP の経路を OSPF に，OSPF の経路を eBGP にそれぞれ再配布を行っていることから，経路情報のループを防止するために，eBGP 接続でプレフィックスリストによる経路フィルタリングを行っている。

・R20，R21 の内部ネットワークと接続するインタフェースでは，PC に設定するデフォルトルートのネクストホップに相当する，［ c ］の可用性を向上するために，VRRP が動作している。

・VRRP のプライオリティの値は R20 を 105 に，R21 を 100 に設定している。

・VRRP はプリエンプトを設定し，プライオリティの値が大きいルータが常にマスターになるように制御している。また，③プリエンプトディレイを設定し，プライオリティの値が高いルータの電源をオンにした際や再起動した際などは，一定時間が経過した後にマスターに状態遷移するように制御している。

〔ルータ更改手順の作成〕

更改対象のルータは，図 1 中の R10，R11，R20，R21，R30，R31 である。A 社情報システム部の D 課長は，次の方針に従ってルータ更改手順を作成するように B さんに指示した。

・更改対象のルータは，同じルータメーカーの後継機種と交換を行う。後継機種は，更改対象のルータから取得した設定内容で動作することが保証されている。

・更改対象のルータを停止しても業務影響がないよう，あらかじめ設定変更によって通信が更改対象のルータを迂回（うかい）するようにしてからルータを停止し，交換作業を行う。

・交換作業後は，必要な確認を行った後に，設定変更によって通信の迂回を解除す

る。

B さんは方針に従って，ネットワークシミュレーターを使って動作確認をしながら，ルータ更改手順を作成した。ネットワークシミュレーターはメーカーから提供されているソフトウェア製品であり，A 社 NW と同等の環境を PC で仮想的に再現できる。

B さんは，R10 を後継機種の新しい R10（以下，新 R10 という）に更改する手順を作成した。B さんは，④更改手順実施中に業務影響がないことを確認する方法として，内部ネットワークの PC から継続して ping コマンドを実行することにした。また，継続して ping コマンドの結果が正常で，パケットロスが確認されなければ業務影響がないと判断することにした。B さんが作成した R10 の更改手順を表 2 に示す。

表 2　B さんが作成した R10 の更改手順

項番	作業内容
1-1	R10 の⑤ OSPF のコストを変更することで，通信が R10 を迂回するようにする。
1-2	通信が R10 を迂回して正常に行えることを確認する。
1-3	R10 の⑥全ての物理インタフェースを閉塞することで，R10 を A 社 NW から切り離す。
2-1	R10 の設定内容を保存し，手元にコピーを取得して R10 の電源をオフにする。
2-2	R10 の全てのイーサネットケーブルを抜去する。
2-3	R10 の電源ケーブルを抜去し，R10 を事前に設定内容が保存されている新 R10 と交換する。
2-4	新 R10 の電源ケーブルを接続し，新 R10 の電源をオンにする。
2-5	新 R10 の起動後，項番 2-1 で取得した設定内容と比較し，想定外の差分がないことを確認する。
2-6	新 R10 に全てのイーサネットケーブルを接続する。
3-1	新 R10 の全ての物理インタフェースの閉塞を解除する。
3-2	⑦新 R10 から ping コマンドを実行し，結果が正常でパケットロスがないことを確認する。
3-3	新 R10 の OSPF のコストを変更することで，通信の迂回を解除する。
3-4	通信が新 R10 を経由して正常に行えることを確認する。

注記　各項番の作業内容を実施するたびに，継続して実行している ping コマンドの状況を確認する。

B さんは R11，R20，R21，R30，R31 についてもそれぞれの更改手順を作成した。ネットワークシミュレーターを使って，継続して ping コマンドを実行しながらそれぞれの更改手順を実施し，ping コマンドの結果が正常でパケットロスがないことを確認した。更改手順に問題がないことを確認できたので，B さんは更改手順書としてま

とめた。B さんは作成した更改手順書を D 課長に提出し，承認された。

設問 1　〔現在の A 社 NW〕について答えよ。

(1)　本文中の［　a　］～［　c　］に入れる適切な字句を答えよ。

(2)　本文中の下線①について，OSPF のネイバー認証によって，どのような問題を防止することができるか。経路交換の安全性の観点から 35 字以内で答えよ。

(3)　本文中の下線②について，R31 が経路広告する AS_PATH 長は R30 と比較してどうする必要があるか，答えよ。

(4)　本文中の下線③について，ルータの電源をオンにした際や再起動した際に一定時間待つのは，ルータがどのような状態になることを待つためか。OSPF を利用していることに着目して 25 字以内で答えよ。

設問 2　〔ルータ更改手順の作成〕について答えよ。

(1)　本文中の下線④について，R10 の更改手順実施中に，大阪本社の内部ネットワークから ping コマンドを実行する際の宛先にすべき対象と，東京支社の内部ネットワークから ping コマンドを実行する際の宛先にすべき対象を，R10 を経由する通信に着目して，図 1 中の(ア)～(ウ)の記号で全て答えよ。

(2)　表 2 中の下線⑤について，R10 のインタフェースに設定する OSPF のコストをどのような値に変更すべきか。30 字以内で答えよ。

(3)　表 2 中の下線⑥について，項番 2-1 の電源をオフする前に全ての物理インタフェースを閉塞する理由を 30 字以内で答えよ。

(4)　表 2 について，項番 2-6 のイーサネットケーブルを接続する際に，誤ったインタフェースに接続しないようにするために，項番 2-2 の前にどのような手順を追加するべきか。25 字以内で答えよ。

(5)　表 2 中の下線⑦について，新 R10 から ping コマンドを実行する際の宛先にすべき対象を，図 1 中の機器名を用いて四つ答えよ。

問２　ネットワークの改善に関する次の記述を読んで，設問に答えよ。

私立Ｕ中学校（以下，Ｕ校という）では，600 台の PC をＵ校のネットワークに接続してＳ社の教育支援サービス(以下，E サービスという)を利用している。Ｕ校では最近校内サービスの不具合に関する申告が多くの生徒から挙がってきたので，Ｕ校は本ネットワークを設計，構築したＴ社に調査を依頼し，Ｔ社のＶさんが担当になった。

〔Ｕ校ネットワークの概要〕

ＶさんはＵ校ネットワーク構成を確認した。Ｕ校ネットワーク構成を図１に示す。

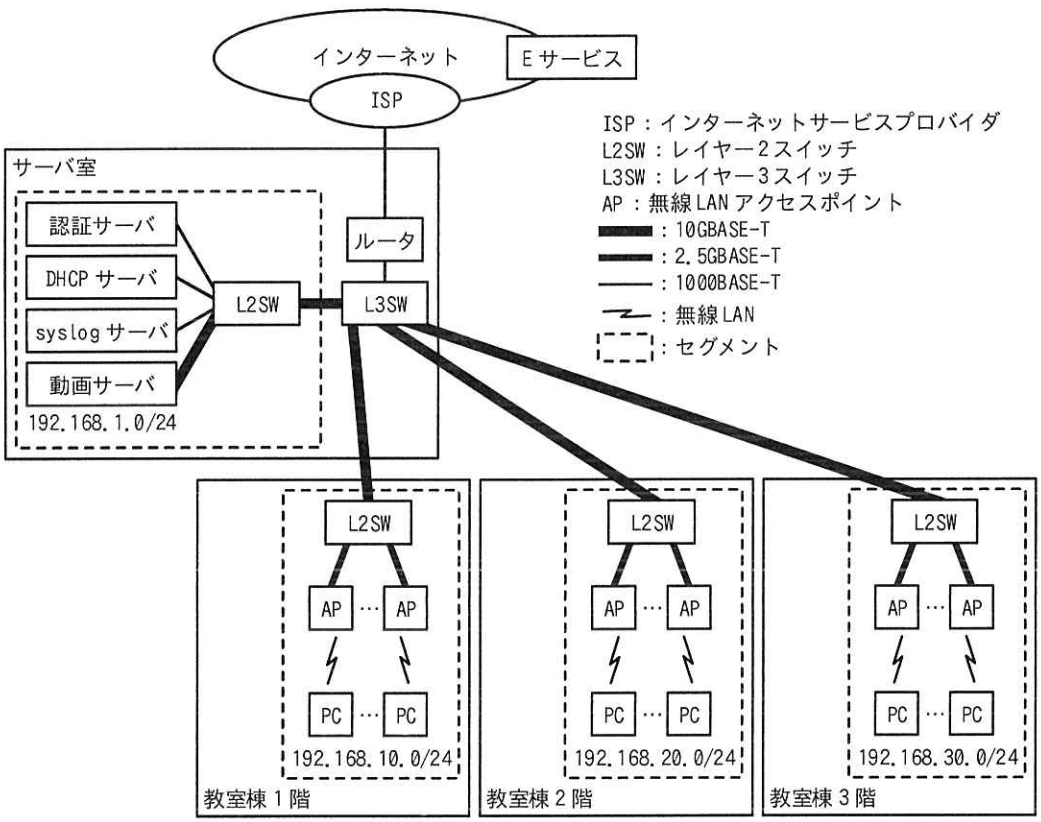


図１　Ｕ校ネットワーク構成

・ISP との接続は，最大１Ｇビット／秒のベストエフォート型インターネット接続サービスを契約して利用している。

・ルータは ISP と接続しており，校内からインターネットへのアクセスに対し，NAPT を使って内部の［ a ］IP アドレスを ISP から割り当てられた［ b ］IP アドレスに変換している。この変換情報はルータの NAT 変換テーブルに NAPT 変換エントリーとして格納されている。

・U 校内及び ISP 接続のルーティングは全てスタティックルーティングである。

・AP は Wi-Fi 6 に対応しており，各教室に 1 台ずつ設置されている。L2SW は，最大 30 W を給電する［ c ］機能をもち，イーサネットケーブル経由で AP に電力を供給している。

・PC は，認証サーバによって IEEE802.1X 認証を行った上で，AP を介して U 校ネットワークに接続している。

・DHCP サーバは，U 校ネットワークに接続した PC に IP アドレスやサブネットマスクなどを配布している。L3SW には DHCP リレーエージェントが設定されており，PC から送信された DHCPDISCOVER メッセージを DHCP サーバに中継している。①そのときに DHCP リレーエージェントは，giaddr フィールドに DHCPDISCOVER メッセージを受信したインタフェースの IP アドレスを格納している。

・全てのネットワーク機器は，syslog サーバにシステムログを送信している。

・E サービスは，複数のサーバで構成されるクラウド型サービスである。教員及び生徒は，E サービスに PC の Web ブラウザからアクセスしログインして利用している。

・1 か月前から，毎朝始業直後の 8:00～8:15 に E サービスの一つである自習ドリルを用いて全校生徒が一斉に学習している。

・サーバ室の動画サーバには，教職員が管理している複数の教材動画が格納されており，全校生徒が授業や自習のときに PC で視聴している。

〔不具合のヒアリングと調査〕

V さんは，校内サービスの不具合に関する申告について U 校の教職員にヒアリングを行い，次のように整理した。

・E サービスに対し，毎朝の自習ドリルの時間帯にアクセスすると，タイムアウト画面が出てログイン画面が表示されないと，一部かつ不特定の生徒からの申告がある。

・E サービスに対し，毎朝の自習ドリルの時間帯にログインできたが，操作後の応答

が遅いと，複数の生徒からの申告がある。それ以外の時間帯では申告はない。

・校内の動画サーバの教材動画視聴は，時間帯や教室を問わず不具合申告はない。

②これらの結果から，V さんは PC から E サービスにアクセスしたときの，(1)インターネット接続帯域の不足，及び(2)NAPT 処理能力の不足，の二つの仮説を立てた。

(1)インターネット接続帯域の調査

V さんは，U 校の許可を得てルータのインターネット側ポートの通信量データを収集した。インターネット通信量（ダウンロード）を図 2 に示す。

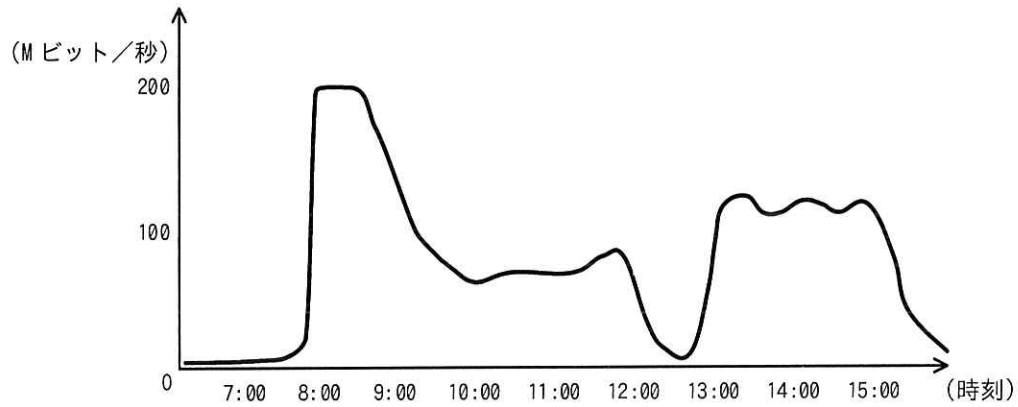


図 2　インターネット通信量（ダウンロード）

図 2 から，実効速度が約 200 M ビット／秒で頭打ちになっていることが判明した。また，この時ルータの CPU 負荷にはまだ余裕があることも確認した。頭打ちの原因を ISP に問い合わせて調査したところ，現在の契約では構成や時間帯によって実効速度はその程度になるとのことだった。V さんは実効速度を改善するために，インターネット接続サービスのベストエフォート型から［　d　］型への契約変更を U 校に紹介することにし，ほかの原因の調査を継続した。

(2)NAPT 処理能力の調査

V さんは，U 校の許可を得て各ネットワーク機器の状態ログ，及び syslog サーバのログを収集し，内容を確認した。ルータの NAT 変換テーブルの状態を表 1 に，ル

ータのシステムログを図3に示す。

表1　ルータのNAT変換テーブルの状態（抜粋）

(i)local IP address	(ii)local port number	(iii)registered IP address	(iv)assigned port number	(v)IP protocol
192.168.10.13	56124	a.b.c.d	5001	udp
192.168.10.22	63219	a.b.c.d	5002	tcp
192.168.20.29	58320	a.b.c.d	5003	udp
⋮	⋮	⋮	⋮	⋮
192.168.30.15	50073	a.b.c.e	5001	tcp
⋮	⋮	⋮	⋮	⋮

a.b.c.d，a.b.c.e：ISPから割り当てられたIPアドレス

```
2025-04-26T08:00:56.52+09:00 IP NAT translation table full (max entries), dropping packet from
192.168.10.102 to f.g.h.i
2025-04-26T08:01:00.66+09:00 IP NAT translation table full (max entries), dropping packet from
192.168.30.29 to f.g.h.i
2025-04-26T08:01:05.23+09:00 IP NAT translation table full (max entries), dropping packet from
192.168.20.19 to f.g.h.i
                                        ⋮
```

f.g.h.i：EサービスのIPアドレス

図3　ルータのシステムログ(抜粋)

表1から，ルータのNAPT変換エントリーの内容には異常は見当たらなかった。また，図3から，始業直後にルータのNAT変換テーブルが枯渇していることが判明した。また，ルータのNAT変換テーブルのエントリー数の上限は65,536であり，設定によって変更することが可能であった。Vさんは，③PC1台当たりのセッション数を最大200と見積もり，全てのPCが問題なく利用できるように，NAT変換テーブルのエントリー数を計算してルータに設定することにした。

〔HTTPバージョンとNAPTとの関係〕

Vさんは，二つの仮説の調査結果をまとめて上司のW課長へ報告した。W課長は，その報告のNAPT処理能力に関しては更なる注意が必要と考え，資料を提示してVさんに説明した。HTTPバージョンとNAPTとの関係を図4に示す。

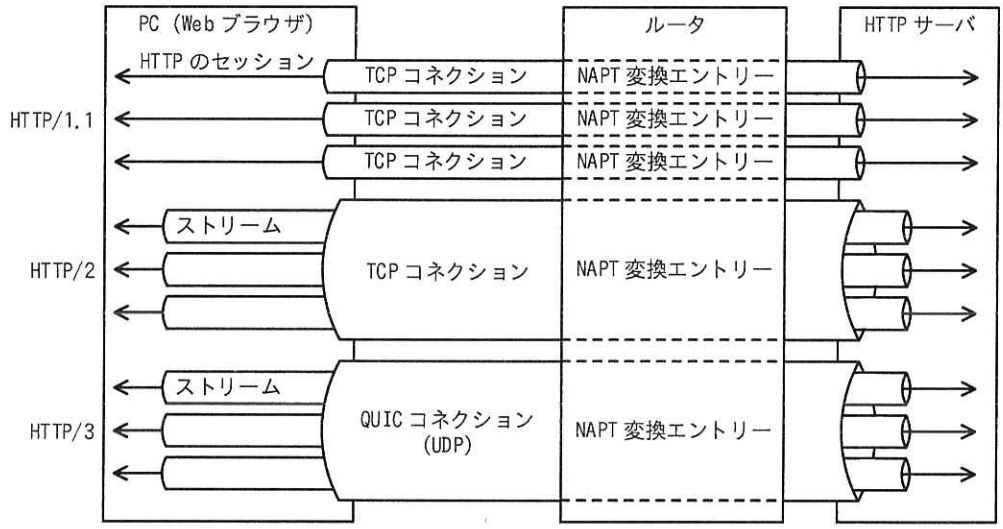


図 4　HTTP バージョンと NAPT との関係

次は W 課長と V さんとの会話である。

W 課長：NAPT 処理能力に着目したようですが，処理能力のほかに HTTP バージョンと NAPT 変換エントリー数との関係も意識しておく必要があると思います。

V さん：HTTP のバージョンが，NAPT 変換エントリー数と何か関係があるのですか。

W 課長：図 4 で説明しましょう。HTTP は長らく HTTP/1.1 が主流でしたが，Web サイトが地図などの詳細画像，動画，アニメーションなどのコンテンツから構成されるようになるにつれて，④ HoL（Head of Line）ブロッキングの問題が表面化してきました。これは一般的に，直列処理の場合，全ての処理が完了するまでに時間が掛かるという問題です。

V さん：HTTP/1.1 では，HoL ブロッキングはどのレイヤーで発生するのですか。

W 課長：HTTP レイヤーと TCP レイヤーの両方で発生します。HTTP レイヤーでは，例えば Web ページの表示のために 10 枚の画像データをダウンロードする場合，PC からの HTTP［　e　］と，それに対するサーバからの HTTP［　f　］を一つずつ 10 回実行することになり時間が掛かるので，一般的には複数の TCP コネクションで同時にダウンロードするように実装して対処します。

V さん：HTTP/1.1 では，TCP コネクションの数が増えそうですね。

W 課長：それを抑えるために，HTTP/2 では仮想的な通信単位であるストリームの概念が導入されました。ストリームにはそれぞれ［　g　］が付与され，一つ

のTCPコネクションの中で複数のストリームを利用できるようになり，HTTPセッションの多重化と［　h　］処理ができるようになっています。

Vさん：HTTP/2によってTCPコネクションの数も少なくて済むようですね。

W課長：さらにHTTP/3では，TCPの代わりにUDPを利用し，ストリームはQUICで実現することで，TCPレイヤーのHoLブロッキングの問題を回避しています。最近のWebブラウザの多くはHTTP/3を実装しているので，どのHTTPバージョンが使われるかは主にHTTPサーバ側の実装に依存すると考えられます。

Vさん：つまり，TCPとUDPそれぞれに対するルータのNAT変換テーブルの管理方法の違いと，Eサービスで利用可能なHTTPバージョンが分かれば，もっと改善できるということですね。

W課長：そうです。今回のケースでは，⑤Eサービスのサーバがもし HTTP/3 に対応していれば，表2の保持時間を調整することで，もっとNAT変換テーブルを有効活用できると思います。ただし，極端な値にすると別の問題が発生するので，気を付けてください。

Vさん：分かりました。検討してみます。

表2　現在のルータのNAPT変換エントリー保持時間

通信プロトコル	保持時間
TCP（SYN）	30秒
TCP（FIN又はRST片方向）	60秒
TCP（FIN又はRST双方向）	1秒
UDP	300秒
DNS	60秒
ICMP	60秒

保持時間：無通信状態のNAPT変換エントリーを保持する時間

Vさんは，調査結果をU校に報告した。その後U校で対策を行い，不具合は解決した。

設問1　〔U校ネットワークの概要〕について答えよ。

(1)　本文中の［　a　］～［　c　］に入れる適切な字句を答えよ。

(2)　本文中の下線①について，DHCPサーバは受け取ったgiaddrフィールドの

情報を使って何を識別するかを，15 字以内で答えよ。

設問２　〔不具合のヒアリングと調査〕について答えよ。

(1)　本文中の下線②について，V さんがインターネット接続帯域の不足だけではなく，NAPT 処理能力の不足という仮説を立てた理由を，40 字以内で答えよ。

(2)　本文中の［　d　］に入れる適切な字句を答えよ。

(3)　表 1 について，NAPT 変換エントリーを作成する際に，ルータ自身が割り当てている値を，(ｉ)～(ｖ)の記号で全て答えよ。

(4)　本文中の下線③について，現状の設定で問題なく同時利用できる PC 台数の上限を，整数で答えよ。また，全ての PC が問題なく同時利用するために，ルータの NAT 変換テーブルのエントリー数を最低幾つ以上に設定すればよいかを，整数で答えよ。ここで，PC 以外の通信は考慮しないものとする。

設問３　〔HTTP バージョンと NAPT との関係〕について答えよ。

(1)　本文中の下線④について，全ての処理が完了するまでに時間が掛かる理由を，30 字以内で答えよ。

(2)　本文中の［　e　］～［　h　］に入れる適切な字句を答えよ。

(3)　本文中の下線⑤の保持時間の調整について，どの通信プロトコルをどのように変更するか，25 字以内で答えよ。また，それによる効果を 45 字以内で答えよ。

問３　セキュア Web ゲートウェイの導入に関する次の記述を読んで，設問に答えよ。

J 社は従業員 50 名の部品メーカーである。J 社では PC の Web ブラウザを利用して，社内の業務用サーバ，K 社が提供する電子メール・ストレージサービス（以下，K 社 SaaS という）に HTTPS でアクセスして業務を行っている。このたび，テレワーク勤務の導入，プロキシサーバの運用作業の省力化及びセキュリティ強化のため，L 社が提供するセキュア Web ゲートウェイサービス（以下，SWG サービスという）を導入することになり，その担当として情報システム部の C 主任が任命された。

〔J 社のネットワーク構成〕

J 社のネットワークは，DMZ セグメント（以下，DMZ という），サーバセグメント及び内部セグメントから構成されている。現状の J 社のネットワーク構成を図 1 に示す。

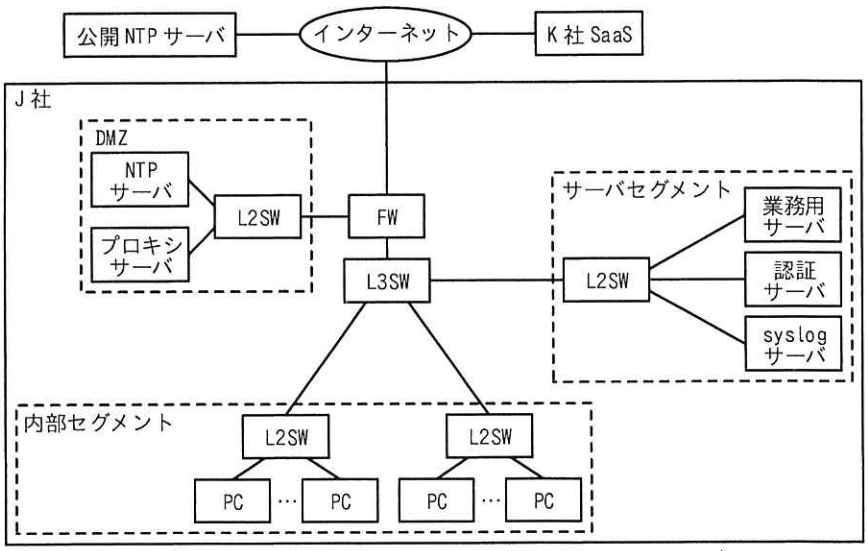


図 1　現状の J 社のネットワーク構成

K 社 SaaS は，電子メールの送受信，ファイルの保存・参照・ダウンロードの機能を提供している。K 社 SaaS では，アクセスを許可する送信元を J 社のグローバル IP アドレスだけに制限し，利用時は利用者認証を行っている。

DMZ には，NTP サーバ及びプロキシサーバが設置されている。NTP サーバはプロバイダが提供する公開 NTP サーバと時刻同期しており，①社内のネットワーク機器，サーバ及び PC の時刻補正に利用されている。プロキシサーバは PC からインターネットへのアクセスに対して，登録した FQDN や IP アドレス宛ての通信をブロックする。PC のプロキシ設定は PAC ファイルを利用して，②インターネット上の Web サイトへはプロキシサーバを経由し，業務用サーバや K 社 SaaS へはプロキシサーバを経由せずに直接接続する設定としている。プロキシサーバは TCP/10080 で接続を待ち受ける設定にしている。

内部セグメントには，PC が設置されており，L3SW のもつ DHCP サーバ機能で IP アドレスなどが割り当てられている。

サーバセグメントには，業務用サーバ，認証サーバ及び syslog サーバが設置されている。認証サーバは，プロキシサーバ及び業務用サーバの接続時に RADIUS プロトコルを用いて利用者認証を行っている。syslog サーバは，③プロキシサーバ及び業務用サーバのアクセスログ，認証サーバの認証ログ，FW の通信ログ，L3SW の DHCP リースログ，J 社内のサーバやスイッチのシステムログを保存している。syslog サーバに保存しているログは，業務用サーバや Web サイトへのアクセス履歴の確認，障害発生時の原因分析に利用されている。

J 社のネットワークからインターネットには，FW がもつキャッシュ DNS サーバ及び NAPT の機能を利用してアクセスしている。FW の許可ルールを表 1 に示す。

表 1　FW の許可ルール（抜粋）

項番	送信元	宛先	プロトコル/宛先ポート番号
1	DMZ	a	UDP/514
2	プロキシサーバ	インターネット	TCP/80, TCP/443
3	プロキシサーバ	b	UDP/1812
4	NTP サーバ	公開 NTP サーバ	UDP/123
5	サーバセグメント	NTP サーバ	UDP/123
6	内部セグメント	NTP サーバ	UDP/123
7	内部セグメント	プロキシサーバ	TCP/ c
8	内部セグメント	K 社 SaaS	TCP/ d

注記　FW は応答パケットを自動的に通過させるステートフルパケットインスペクション機能をもつ。

〔SWG サービスの仕様調査〕

C 主任は SWG サービスの仕様を調査した。

SWG サービスは，セキュリティ機能及びプロキシ機能をもつクラウド型のサービスである。PC にエージェントソフト（以下，ソフト E という）を導入し，Web ブラウザからソフト E 及び SWG サービスを経由して Web サイトにアクセスする。④SWG サービスは HTTPS 通信のコンテンツを調査する機能をもつ。SWG サービスを経由して Web サイトにアクセスする HTTPS 通信を信頼させるために，PC に証明書をあらかじめインストールする。

SWG サービスは，一部の Web サイトで実施される送信元アドレス制限に対応するため，契約した企業単位に固定のグローバル IP アドレス（以下，SWG-GIP という）を割り当てるサービスメニューをもつ。契約した企業の通信を SWG サービスが中継する際，送信元アドレスを SWG-GIP に変換する。

ソフト E を導入すると，PC のプロキシ設定が変更され，プロキシサーバとしてソフト E が設定される。ソフト E は PC のローカルプロキシとして動作し，HTTP 及び HTTPS の通信を SWG サービスの TCP/443 ポート宛てに中継する。ソフト E は SWG サービスに登録された直接接続リストをダウンロードして，このリストに登録された Web サイトには SWG サービスを経由させずに，ソフト E から直接接続する。ソフト E は，SWG サービスにアクセスするときに利用者認証を行い，認証に失敗した場合又は未認証の場合，ソフト E 及び SWG サービスは HTTP 及び HTTPS の通信をブロックする。

SWG サービスのセキュリティ機能を表 2 に示す。

表 2　SWG サービスのセキュリティ機能（抜粋）

機能名	機能概要
ダイレクト通信機能	直接接続リストに登録した FQDN，IP アドレスを宛先とする通信は，SWG サービスを経由させずに直接通信させる機能
サイトブロック機能	拒否リストに登録した FQDN，IP アドレス又は URL を宛先とする通信をブロックする機能
レピュテーション機能	接続先のドメインや IP アドレスの安全性を数値化し，指定したしきい値以上の安全性をもつ Web サイトだけに接続を許可する機能
マルウェア駆除機能	ダウンロード・アップロードファイルに対して，パターン検査及び⑤隔離環境上で動作を観察・分析してマルウェアを駆除する機能

〔導入検討〕

C 主任は，SWG サービスの導入に向けて，F 課長と検討を行った。

F 課長：まずは，社内ネットワークの変更点を説明してください。

C 主任：PC から SWG サービスを利用するため，全ての PC にソフト E を導入します。これによって，社内で利用する PC 及びテレワーク勤務のために社外に持ち出した PC（以下，R-PC という）からのアクセスが，SWG サービスを経由するようになります。SWG サービスのサービスメニューを利用して，SWG-GIP を割り当ててもらいます。また，R-PC から業務用サーバに接続できるように，現在利用している社内のプロキシサーバは，設定を変更してフォワードプロキシサーバからリバースプロキシサーバに利用方法を変更します。⑥フォワードプロキシサーバの機能停止に伴って FW の許可ルールを削除し，リバースプロキシサーバのために許可ルールを追加します。

F 課長：SWG サービスを導入した場合，社内の PC から K 社 SaaS へのアクセス経路を教えてください。

C 主任：SWG サービス導入時のネットワーク構成を図 2 に示します。図 2 の⑦ (G)，(F)，(I)，(H)，(J)の経路になります。

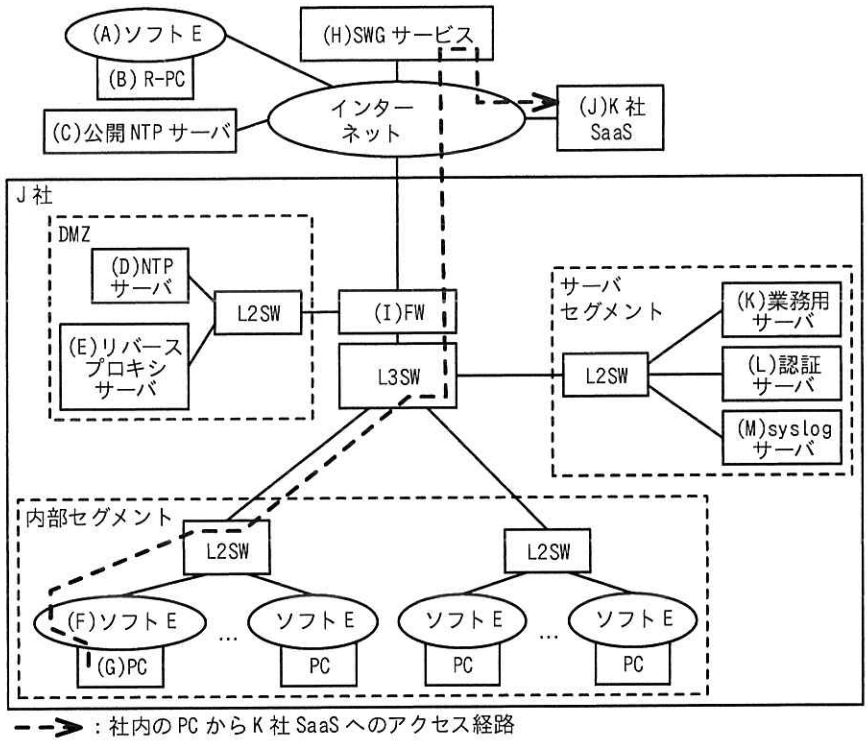


図 2　SWG サービス導入時のネットワーク構成

F 課長：FW に，⑧ PC が SWG サービスへ接続するための許可ルールが必要ですね。次に SWG サービスのセキュリティ機能の利用方針を説明してください。

C 主任：サイトブロック機能には，フォワードプロキシサーバでブロック先として登録していた FQDN や IP アドレスを設定します。レピュテーション機能では，安全性が高い Web サイトだけに接続させるため，導入時はできるだけしきい値を高く設定しておき，業務影響を確認しながら調整していきます。

F 課長：現在は，PC から業務用サーバ及び K 社 SaaS には直接接続していますが，SWG サービスを導入した場合にダイレクト通信機能は利用しないのですか。

C 主任：業務用サーバ及び K 社 SaaS には，SWG サービスを経由して通信させるため，ダイレクト通信機能は利用しない予定です。併せて，⑨ K 社 SaaS の設定を変更します。また，業務用サーバへ SWG サービスからの通信を FW で許可します。

F 課長：なるほど。PC，R-PC どちらも SWG サービスを経由させてセキュリティポリシーを合わせていますが，⑩通信の経路を考慮すると業務用サーバのプライベート IP アドレスは直接接続リストに登録した方が良いですね。

C 主任：分かりました。業務用サーバのプライベート IP アドレスを直接接続リストに登録します。

F 課長：SWG サービスは 90 日間のトライアル利用ができるので，機能確認や移行方法を検討してください。

C 主任はトライアルの結果を基に，SWG サービスの導入計画を立案し，承認された。

設問 1　〔J 社のネットワーク構成〕について答えよ。

(1)　本文中の下線①について，複数機器の時刻を補正する目的を，ログ解析に着目して 25 字以内で答えよ。

(2)　本文中の下線②について，J 社がプロキシサーバを経由させる目的を，本文中の字句を用いて二つ挙げ，それぞれ 35 字以内で答えよ。

(3)　本文中の下線③のうち，FW の通信ログにおいて，PC からの不正な通信が確認された後で PC を特定するために確認するログを本文中の字句で答えよ。

(4) 表 1 中の［ a ］，［ b ］に入れる適切な機器名を，図 1 中の字句で答えよ。

(5) 表 1 中の［ c ］，［ d ］に入れる適切な数字を答えよ。

設問２ 〔SWG サービスの仕様調査〕について答えよ。

(1) 本文中の下線④について，あらかじめ PC にインストールする証明書を 20 字以内で答えよ。

(2) 表 2 中の下線⑤について，ファイルが遠隔操作可能なマルウェアを含む場合，隔離環境上での動作時に観察される外部通信先の名称を答えよ。

設問３ 〔導入検討〕について答えよ。

(1) 本文中の下線⑥の機能停止に伴って削除する許可ルールを，表 1 中の項番 1～8 から二つ選んで数字で答えよ。

(2) (B) R-PC から(K)業務用サーバに接続する場合のアクセス経路を，図 2 中の(A)～(M)を用いて，本文中の下線⑦の記述に従って答えよ。

(3) 本文中の下線⑧について，FW に追加する許可ルール（送信元，宛先，プロトコル/宛先ポート番号）を答えよ。

(4) 本文中の下線⑨について，K 社 SaaS の設定の変更内容を 35 字以内で答えよ。

(5) 本文中の下線⑩によって得られる利点を，通信の経路に着目して 10 字以内で答えよ。

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

6. 退室可能時間中に退室する場合は，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	13:10 ～ 13:50

7. **問題に関する質問にはお答えできません。**文意どおり解釈してください。
8. 問題冊子の余白などは，適宜利用して構いません。ただし，問題冊子を切り離して利用することはできません。
9. 試験時間中，机上に置けるものは，次のものに限ります。

   なお，会場での貸出しは行っていません。

   受験票，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（時計型ウェアラブル端末は除く。アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬

   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
12. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。
13. 午後 II の試験開始は 14:30 ですので，14:10 までに着席してください。