正　誤　表

令和4年4月17日実施

ネットワークスペシャリスト試験　午後Ⅰ　問題

ページ	問題番号	行	誤	正	訂正の内容
11	2	図2 下から 2行目	…P 社営業支援システムを利用する際に …	…P 社営業支援サービスを利用する際に …	下線部分を訂正する。

問2　セキュアゲートウェイサービスの導入に関する次の記述を読んで，設問 1～3 に答えよ。

N 社は，国内に本社及び一つの営業所をもつ，中堅の機械部品メーカである。従業員は，N 社が配布する PC を本社又は営業所の LAN に接続して，本社のサーバ，及び SaaS として提供される P 社の営業支援サービスを利用して業務を行っている。

N 社は，クラウドサービスの利用を進め，従業員のテレワーク環境を整備することにした。N 社の情報システム部は，本社のオンプレミスのサーバから Q 社の PaaS への移行と，Q 社のセキュアゲートウェイサービス（以下，SGW サービスという）の導入を検討することになった。SGW サービスは，PC がインターネット上のサイトに接続する際に，送受信するパケットを本サービス経由とすることによって，ファイアウォール機能などの情報セキュリティ機能を提供する。

〔現行のネットワーク構成〕

N 社の現行のネットワーク構成を図 1 に示す。

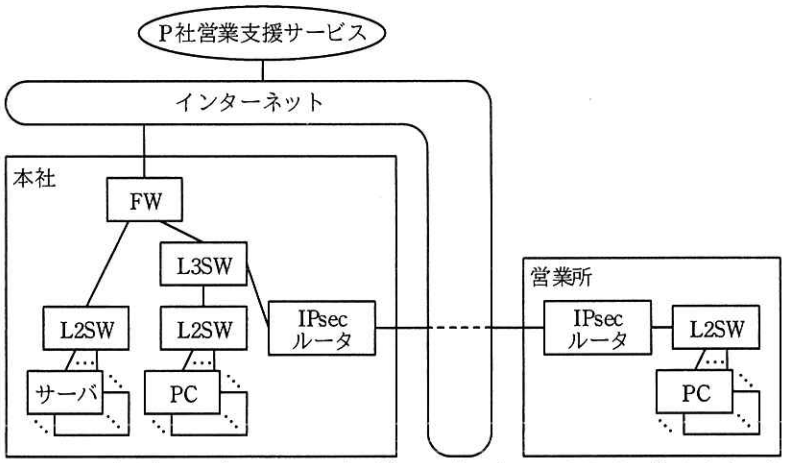


図 1　N 社の現行のネットワーク構成（抜粋）

N 社の現行システムの概要を次に示す。

・本社及び営業所の LAN は，IPsec ルータを利用した IPsec VPN で接続している。

・本社及び営業所の IPsec ルータは，IPsec VPN を確立したときに有効化される仮想インタフェース（以下，トンネル IF という）を利用して相互に接続する。
・営業所の PC から P 社営業支援サービス宛てのパケットは，営業所の IPsec ルータ，本社の IPsec ルータ，L3SW，FW 及びインターネットを経由して P 社営業支援サービスに送信される。
・FW は，パケットフィルタリングによるアクセス制御と，NAPT による IP アドレスの変換を行う。
・P 社営業支援サービスでは，①特定の IP アドレスから送信されたパケットだけを許可するアクセス制御を設定して，本社の FW を経由しない経路からの接続を制限している。

本社及び営業所の IPsec ルータは，LAN 及びインターネットのそれぞれでデフォルトルートを使用するために，VRF（Virtual Routing and Forwarding）を利用して二つの［ a ］テーブルを保持し，経路情報を VRF の識別子（以下，VRF 識別子という）によって識別する。ネットワーク機器の VRF とインタフェース情報を表 1 に，ネットワーク機器に設定している VRF と経路情報を表 2 に示す。

表 1　ネットワーク機器の VRF とインタフェース情報（抜粋）

拠点	機器名	VRF 識別子	インタフェース	IP アドレス	サブネットマスク	接続先
本社	FW	－	INT-IF 1)	a.b.c.d 3)	（省略）	ISP のルータ
			LAN-IF 2)	172.16.0.1	255.255.255.0	L3SW
	IPsec ルータ	65000:1	INT-IF 1)	s.t.u.v 3)	（省略）	ISP のルータ
		65000:2	LAN-IF 2)	172.17.0.1	255.255.255.0	L3SW
			トンネル IF	（省略）	（省略）	営業所の IPsec ルータ
営業所	IPsec ルータ	65000:1	INT-IF 1)	w.x.y.z 4)	（省略）	ISP のルータ
		65000:2	LAN-IF 2)	172.17.1.1	255.255.255.0	L2SW
			トンネル IF	（省略）	（省略）	本社の IPsec ルータ

注 1)　INT-IF は，インターネットに接続するインタフェースである。
注 2)　LAN-IF は，本社又は営業所の LAN に接続するインタフェースである。
注 3)　a.b.c.d 及び s.t.u.v は，固定のグローバル IP アドレスである。
注 4)　w.x.y.z は，ISP から割り当てられた動的なグローバル IP アドレスである。

表2　ネットワーク機器に設定しているVRFと経路情報（抜粋）

拠点	機器名	VRF識別子	宛先ネットワーク	ネクストホップとなる装置又はインタフェース	経路制御方式
本社	FW	－	0.0.0.0/0	ISPのルータ	静的経路制御
			172.17.1.0/24（営業所のLAN）	本社のL3SW	動的経路制御
	IPsecルータ	65000:1	0.0.0.0/0	ISPのルータ	静的経路制御
		65000:2	0.0.0.0/0	b	動的経路制御
			172.17.1.0/24（営業所のLAN）	トンネルIF	c
営業所	IPsecルータ	65000:1	0.0.0.0/0	ISPのルータ	静的経路制御
		65000:2	0.0.0.0/0	トンネルIF	d

N社のネットワーク機器に設定している経路制御を，次に示す。

・本社のFW，L3SW及びIPsecルータには，OSPFによる経路制御を稼働させるための設定を行っている。

・本社のFWには，OSPFにデフォルトルートを配布する設定を行っている。

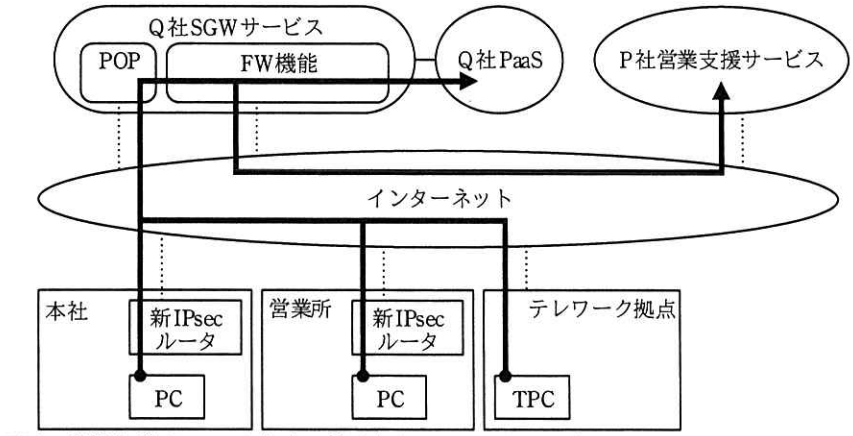
・②本社のIPsecルータには，営業所のIPsecルータとIPsec VPNを確立するために，静的なデフォルトルートを設定している。

・本社及び営業所のIPsecルータには，営業所のPCが通信するパケットをIPsec VPNを介して転送するために，トンネルIFをネクストホップとした静的経路を設定している。

・本社のIPsecルータには，OSPFに③静的経路を再配布する設定を行っている。

〔新規ネットワークの検討〕

Q社のPaaS及びSGWサービスの導入は，N社の情報システム部のR主任が担当することになった。R主任が考えた新規ネットワーク構成と通信の流れを図2に示す。



TPC：従業員がテレワーク拠点で利用するPC　　POP：Point of Presence

➡：PC及びTPCから，Q社PaaS及びP社営業支援システムを利用する際に発生する通信の流れ

……：インターネットとの接続

図2　R主任が考えた新規ネットワーク構成と通信の流れ（抜粋）

R主任が考えた新規ネットワーク構成の概要を次に示す。

・本社のサーバ上で稼働するシステムを，Q社PaaSへ移行する。

・Q社SGWサービスを利用するために，本社及び営業所に導入する新IPsecルータ，並びにTPCは，Q社SGWサービスのPOPという接続点にトンネルモードのIPsec VPNを用いて接続する。

・PC及びTPCからP社営業支援サービス宛てのパケットは，Q社SGWサービスのPOPとFW機能及びインターネットを経由してP社営業支援サービスに送信される。

・Q社SGWサービスのFW機能は，パケットフィルタリングによるアクセス制御と，NAPTによるIPアドレスの変換を行う。

R主任は，POPとの接続に利用するIPsec VPNについて，検討した。

IPsec VPNには，IKEバージョン2と，ESPのプロトコルを用いる。新IPsecルータ及びTPCとPOPは，IKE SAを確立するために必要な，暗号化アルゴリズム，疑似ランダム関数，完全性アルゴリズム及びDiffie-Hellmanグループ番号を，ネゴシエーションして決定し，IKE SAを確立する。次に，新IPsecルータ及びTPCとPOPは，認証及びChild SAを確立するために必要な情報を，IKE SAを介してネゴシエーションして決定し，Child SAを確立する。

新 IPsec ルータ及び TPC は，IPsec VPN を介して転送する必要があるパケットを，長さを調整する ESP トレーラを付加して［ e ］化する。次に，新しい［ f ］ヘッダと，［ g ］SA を識別するための ESP ヘッダ及び ESP 認証データを付加して，POP 宛てに送信する。

R 主任は，IPsec VPN の構成に用いるパラメータについて，現行の設計と比較検討した。検討したパラメータのうち，鍵の生成に用いるアルゴリズムと［ h ］を定めている Diffie-Hellman グループ番号には，現行では 1 を用いているが，POP との接続では 1 よりも［ h ］の長い 14 を用いた方が良いと考えた。

〔接続テスト〕

Q 社の PaaS 及び SGW サービスの導入を検討するに当たって，Q 社からテスト環境を提供してもらい，本社，営業所及びテレワーク拠点から，Q 社 PaaS 及び P 社営業支援サービスを利用する接続テストを行うことになった。

R 主任は，接続テストを行う準備として，P 社営業支援サービスに設定しているアクセス制御を変更する必要があると考えた。P 社営業支援サービスへの接続を許可する IP アドレスには，Q 社 SGW サービスの FW 機能での NAPT のために，Q 社 SGW サービスから割当てを受けた固定のグローバル IP アドレスを設定する。R 主任は，Q 社 SGW サービスが N 社以外にも提供されていると考えて，④NAPT のために Q 社 SGW サービスから割当てを受けたグローバル IP アドレスのサービス仕様を，Q 社に確認した。

テスト環境を構築した R 主任は，Q 社 PaaS 及び⑤P 社営業支援サービスの応答時間の測定を確認項目の一つとして，接続テストを実施した。

R 主任は，N 社の幹部に接続テストの結果に問題がなかったことを報告し，Q 社の PaaS 及び SGW サービスの導入が承認された。

設問 1　〔現行のネットワーク構成〕について，(1)～(6) に答えよ。

(1) 本文中の下線①の IP アドレスを，表 1 中の IP アドレスで答えよ。

(2) 本文中の［ a ］に入れる適切な字句を答えよ。

(3) 表 2 中の［ b ］～［ d ］に入れる適切な字句を，表 2 中の字句を

用いて答えよ。

(4) “本社の IPsec ルータ”が，営業所の PC から P 社営業支援サービス宛てのパケットを転送するときに選択する経路は，表2中のどれか。VRF 識別子及び宛先ネットワークを答えよ。

(5) 本文中の下線②について，デフォルトルート（宛先ネットワーク 0.0.0.0/0 の経路）が必要になる理由を，40 字以内で述べよ。

(6) 本文中の下線③の宛先ネットワークを，表 2 中の字句を用いて答えよ。

設問２ 〔新規ネットワークの検討〕について，(1)，(2) に答えよ。

(1) 本文中の［ e ］～［ h ］に入れる適切な字句を答えよ。

(2) POP との IPsec VPN を確立できない場合に，失敗しているネゴシエーションを特定するためには，何の状態を確認するべきか。本文中の字句を用いて二つ答えよ。

設問３ 〔接続テスト〕について，(1)，(2) に答えよ。

(1) 本文中の下線④について，情報セキュリティの観点で R 主任が確認した内容を，20 字以内で答えよ。

(2) 本文中の下線⑤について，P 社営業支援サービスの応答時間が，現行よりも長くなると考えられる要因を 30 字以内で答えよ。