NW

令和４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〕

選択欄	
２問選択	(問１)
	問２
	(問３)

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。

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1　ネットワークの更改に関する次の記述を読んで，設問1～3に答えよ。

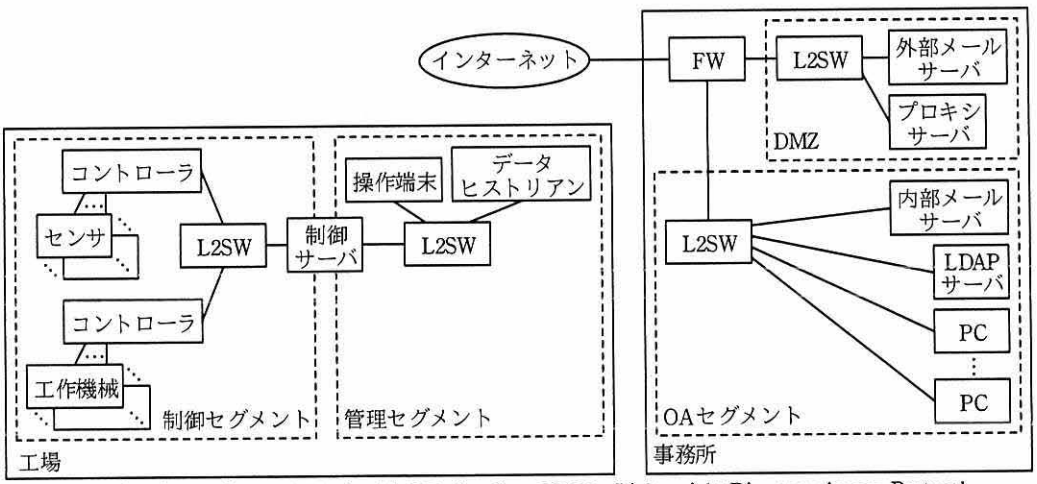
〔現状のネットワーク〕

A社は，精密機械部品を製造する中小企業であり，敷地内に事務所と工場がある。事務所には電子メール（以下，メールという）送受信やビジネス資料作成などのためのOAセグメントと，社外との通信を行うDMZが設置されている。工場には工作機械やセンサを制御するための制御セグメントと，制御サーバと操作端末のアクセスログ（以下，ログデータという）や制御セグメントからの測定データを管理するための管理セグメントが設置されている。

センサや工作機械を制御するコントローラの通信は制御セグメントに閉じた設計としているので，事務所と工場の間は，ネットワークで接続されていない。また制御セグメントと管理セグメントの間には，制御サーバが設置されているがルーティングは行わない。

操作端末は，制御サーバを介してコントローラに対し設定値やコマンドを送出する。コントローラは，常に測定データを制御サーバに送信する。制御サーバは，収集した測定データを，1日1回データヒストリアンに送る。データヒストリアンは，ログデータ及び測定データを蓄積する。

A社ネットワークの構成を，図1に示す。



FW：ファイアウォール　L2SW：レイヤ2スイッチ　LDAP：Lightweight Directory Access Protocol

図1　A社ネットワークの構成（抜粋）

ログデータの転送は，イベント通知を転送する標準規格（RFC 5424）の［ a ］プロトコルを利用している。データヒストリアンに蓄積された測定データとログデータは，ファイル共有プロトコルで操作端末に共有され，社員が USB メモリを用いて OA セグメント内の PC に 1 週間に 1 回複製する。

制御サーバ，操作端末及びデータヒストリアンのソフトウェア更新は，必要の都度，OA セグメントの PC でインターネットからダウンロードしたソフトウェア更新ファイルを，USB メモリを用いて操作端末に複製した上で実施される。

A 社の社員は，PC でメールの閲覧やインターネットアクセスを行う。OA セグメントからインターネットへの通信は DMZ 経由としており，DMZ には社外とのメールを中継する外部メールサーバと，OA セグメントからインターネットへの Web 通信を中継するプロキシサーバがある。DMZ にはグローバル IP アドレスが，OA セグメントにはプライベート IP アドレスがそれぞれ用いられている。

社員のメールボックスをもつ内部メールサーバと，プロキシサーバは，ユーザ認証のために LDAP サーバを参照する。プロキシサーバのユーザ認証には，Base64 でエンコードする Basic 認証方式と，MD5 や SHA-256 でハッシュ化する［ b ］認証方式があるが，A 社では後者の方式を採用している。また，プロキシサーバは，HTTP の［ c ］メソッドでトンネリング通信を提供し，トンネリング通信に利用する通信ポートを 443 に限定する。

〔ネットワークの更改方針〕

A 社では，USB メモリ紛失によるデータ漏えいの防止，測定データのリアルタイムの可視化，及び過去の測定データの蓄積のために，USB メモリの利用を廃止し，工場と事務所をネットワークで接続することにした。A 社技術部の B さんが指示された内容を次に示す。

(a) データヒストリアンにあるログデータを PC にファイル送信できるようにする。また PC にダウンロードしたソフトウェア更新ファイルを操作端末にファイル送信できるようにする。

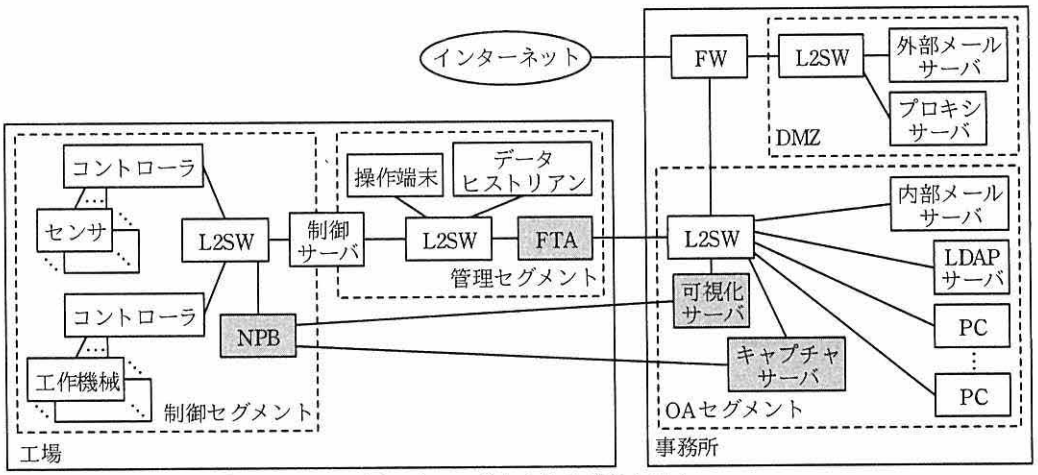
(b) 測定データの統計処理を行い時系列グラフとして可視化するサーバと，長期間の測定データを加工せずそのまま蓄積するサーバを OA セグメントに設置する。

(c) セキュリティ維持のために，工場の制御セグメント及び管理セグメントと，事

務所の OA セグメントとの間はルーティングを行わない。

B さんは，工場のネットワークを設計したベンダに実現方式を相談した。指示 (a) と (c) については，ファイル転送アプライアンス（以下，FTA という）がベンダから提案された。指示 (b) と (c) については，ネットワークパケットブローカ（以下，NPB という），可視化サーバ，キャプチャサーバがベンダから提案された。

B さんがベンダから提案を受けた，A 社ネットワークの構成を，図 2 に示す。



注記　網掛け部分は，ネットワーク更改によって追加される箇所を示す。

図 2　ベンダが提案した A 社ネットワークの構成（抜粋）

〔管理セグメントと OA セグメント間のファイルの受渡し〕

FTA は，分離された二つのネットワークでルーティングすることなくファイルの受渡しができるアプライアンスである。ファイルの送信者は，①FTA に Web ブラウザを使ってログインし，受信者を指定してファイルをアップロードする。ファイルの受信者は，FTA に Web ブラウザを使ってログインし，自身が受信者として指定されたファイルだけをダウンロードできる。

FTA の機能を使い，ファイルの受渡しの際に上長承認手続を必須にする。上長への承認依頼，受信者へのファイルアップロード通知は，FTA が自動的にメールを送信して通知する。承認は設定された上長だけが行うことができる。

B さんが検討した FTA の利用時の流れを，表 1 に示す。

表1　FTAの利用時の流れ

項番	概要	説明
1	アップロード	送信者は，FTA に HTTPS（HTTP over TLS）でアクセスし，PC 又は操作端末から FTA にファイルをアップロードする。
2	承認依頼	上長宛ての承認依頼メールが，FTA から内部メールサーバに自動送信される。
3	承認	上長は，PC でメールを確認後，FTA に HTTPS でアクセスし，ファイルの中身を確認した上で承認する。
4	ファイル アップロード通知	受信者宛てのファイルアップロード通知メールが，FTA から内部メールサーバに自動送信される。
5	ダウンロード	受信者は，PC でメールを確認後，FTA に HTTPS でアクセスし，ファイルを PC 又は操作端末にダウンロードする。

②指示(c)のとおり，FTA には静的経路や経路制御プロトコルの設定は行わない。

③FTA は，認証及び認可に必要な情報について，既存のサーバを参照する。

B さんは，ベンダから FTA を借りて想定どおりに動作をすることを確認した。

〔測定データの可視化〕

NPB は事前に入力ポート，出力ポートを設定し，入力したパケットを複数の出力ポートに複製する装置である。NPB ではフィルタリングを設定して，複製するパケットを絞り込むことができる。可視化サーバは複製されたパケット（以下，ミラーパケットという）を受信して統計処理を行い，時系列グラフによって可視化をすることができる。キャプチャサーバは大容量のストレージをもち，ミラーパケットをそのまま長期間保存することができ，必要時にファイルに書き出すことができる。

B さんは，NPB の動作の詳細についてベンダに確認した。B さんとベンダの会話を次に示す。

B さん：L2SW と NPB の転送方式は，何が違うのですか。

ベンダ：L2SW の転送方式では，受信したイーサネットフレームのヘッダにある送信元 MAC アドレスと L2SW の入力ポートを MAC アドレステーブルに追加します。フレームを転送するときは，宛先 MAC アドレスが MAC アドレステーブルに学習済みかどうかを確認した上で，学習済みの場合には学習されているポートに転送します。宛先 MAC アドレスが学習されていない場合は

[d] します。

これに対して NPB の転送方式では，入力ポートと出力ポートの組合せを事前に定義して通信路を設定します。今回のA社の構成では，一つの入力ポートに対して出力ポートを二つ設定し，パケットの複製を行っています。

NPBの入力は，L2SWからのミラーポートと接続する方法と，ネットワークタップと接続する方法の二つがあります。ネットワークタップは，既存の配線にインラインで接続し，パケットを NPB に複製する装置です。今回検討したネットワークタップを使う方法では，送信側，受信側，それぞれの配線でパケットを複製するので，NPBの入力ポートは2ポート必要です。④今回採用する方法では，想定トラフィック量が少ないので既存のL2SWのミラーポートを用います。NPB につながるケーブルは全て 1000BASE-SX です。

B さんは，ベンダへの確認結果を基に A 社における NPB による測定データの送信について整理した。その内容を次に示す。

・可視化サーバとキャプチャサーバを OA セグメントに設置する。
・コントローラは，更改前と同様に測定データを制御サーバに常時送信する。
・⑤制御セグメントに設置されている L2SW の特定ポートにミラー設定を行い，L2SW の該当ポートの送信側，受信側，双方のパケットを複製して NPB に送信させる。
・NPB は受信したミラーパケットを必要なパケットだけにフィルタリングした後に再度複製し，⑥可視化サーバとキャプチャサーバに送信する。

B さんは，FTA，NPB によるネットワーク接続方式を上司に説明し，承認を得た。

設問1　〔現状のネットワーク〕について，(1)，(2) に答えよ。

(1) 本文中の [a] ～ [c] に入れる適切な字句を答えよ。

(2) 外部からアクセスできるサーバを FW によって独立した DMZ に設置すると，OA セグメントに設置するのに比べて，どのようなセキュリティリスクが軽減されるか。40 字以内で答えよ。

設問2　〔管理セグメントと OA セグメント間のファイルの受渡し〕について，(1)～(3) に答えよ。

(1) 本文中の下線①について，利用者の認証を既存のサーバで一元的に管理する場合，どのサーバから認証情報を取得するのが良いか。図 2 中の字句を用いて答えよ。

(2) 本文中の下線②について，FTA にアクセスできるのはどのセグメントか。図 2 中の字句を用いて全て答えよ。

(3) 本文中の下線③について，FTA において認証と認可はそれぞれ何をするために使われるか。違いが分かるようにそれぞれ 25 字以内で述べよ。

設問3　〔測定データの可視化〕について，(1)～(5) に答えよ。

(1) 本文中の［ d ］に入れる適切な字句を答えよ。

(2) 本文中の下線④について，L2SW からミラーパケットで NPB にデータを入力する場合，ネットワークタップを用いて NPB にデータを入力する方式と比べて，性能面でどのような制約が生じるか。40 字以内で述べよ。

(3) 本文中の下線⑤について，1 ポートだけからミラーパケットを取得する設定にする場合には，どの装置が接続されているポートからミラーパケットを取得するように設定する必要があるか。図 2 中の字句を用いて答えよ。

(4) 本文中の下線⑥について，サーバでミラーパケットを受信するためにはサーバのインタフェースを何というモードに設定する必要があるか答えよ。また，このモードを設定することによって，設定しない場合と比べどのようなフレームを受信できるようになるか。30 字以内で答えよ。

(5) キャプチャサーバに流れるミラーパケットが平均 100 k ビット／秒であるとき，1,000 日間のミラーパケットを保存するのに必要なディスク容量は何 G バイトになるか。ここで，1 k ビット／秒は 10^3 ビット／秒，1 G バイトは 10^9 バイトとする。ミラーパケットは無圧縮で保存するものとし，ミラーパケット以外のメタデータの大きさは無視するものとする。

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。

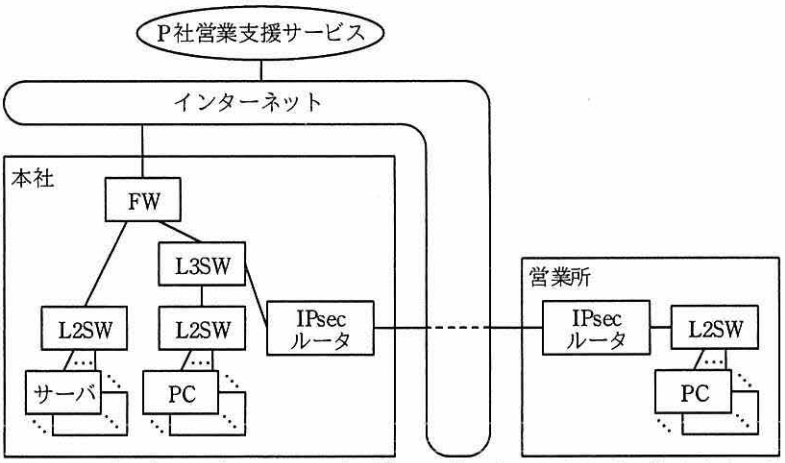


図 1　N 社の現行のネットワーク構成（抜粋）

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。

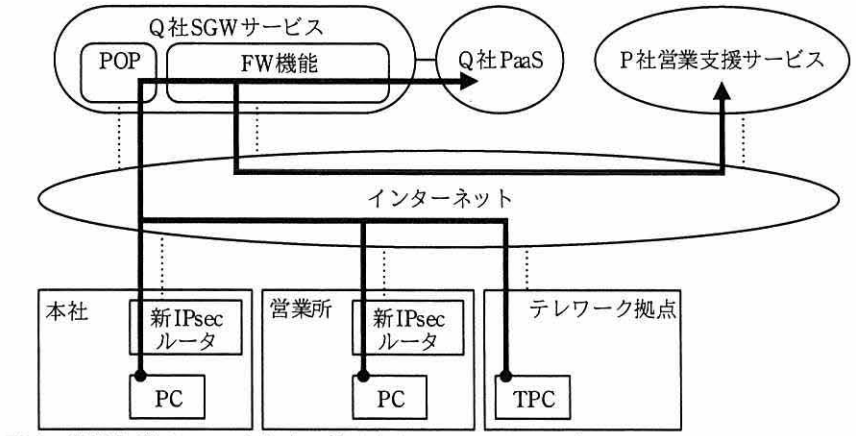
・②本社のIPsecルータには，営業所のIPsecルータとIPsec VPNを確立するために，静的なデフォルトルートを設定している。

・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。

問3　シングルサインオンの導入に関する次の記述を読んで，設問1～3に答えよ。

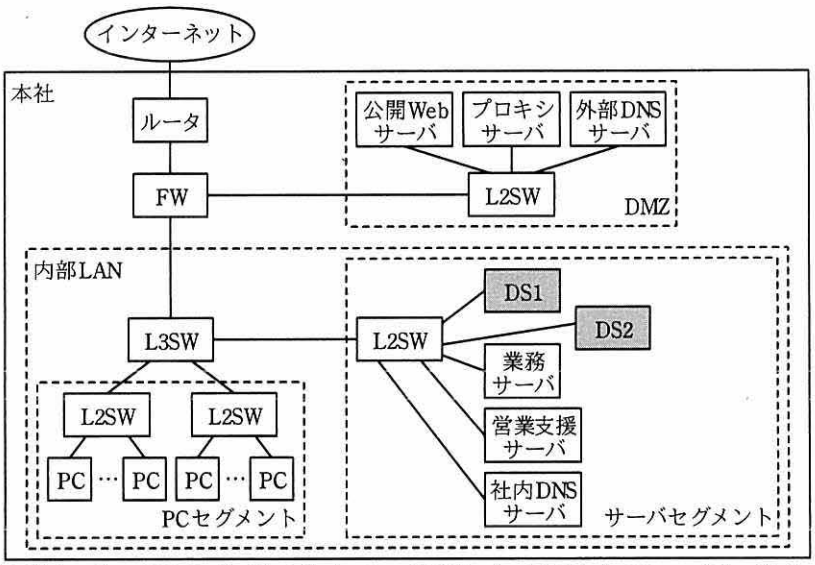
Y社は，医療機器販売会社であり，都内に本社を構えている。受発注業務システムのサーバ（以下，業務サーバという），営業活動支援システムのサーバ（以下，営業支援サーバという）など，複数のサーバを本社で運用している。

Y社では，IT活用の推進によって社員が利用するシステムが増加した結果，パスワードの使い回しが広がり，セキュリティリスクが増大した。また，サーバの運用を担当する情報システム部（以下，情シスという）では，アカウント情報の管理作業が増大したことから，アカウント情報管理の一元化が課題になった。

このような状況から，Y社は，社内のシステムへのシングルサインオン（以下，SSOという）の導入を決定した。情シスのZ課長は，SSOの導入検討を部下のX主任に指示した。

〔ネットワーク構成及び機器の設定と利用形態〕

最初に，X主任は，本社のネットワーク構成及び機器の設定と利用形態をまとめた。X主任が作成した，本社のネットワーク構成を図1に示す。



FW：ファイアウォール　L2SW：レイヤ2スイッチ　L3SW：レイヤ3スイッチ　DS：ディレクトリサーバ
注記　網掛け部分は，アカウント情報の一元管理のために，今後導入予定の機器を示す。

図1　本社のネットワーク構成（抜粋）

現状の機器の設定と利用形態を次に示す。

(i) 社内DNSサーバは，内部LANのゾーン情報を管理し，内部LAN以外のゾーンのホストの名前解決要求は，外部DNSサーバに転送する。

(ii) 外部DNSサーバは，DMZのゾーン情報の管理及びフルサービスリゾルバの機能をもっている。外部DNSサーバは，社外からの再帰問合せ要求は受け付けない。一方，社内DNSサーバ及びDMZのサーバからの再帰問合せ要求は受け付け，再帰問合せ時には，送信元ポート番号のランダム化を行う。

(iii) PCには，プロキシ設定でプロキシサーバのFQDNが登録されているが，(a)業務サーバ及び営業支援サーバへのアクセスは，プロキシサーバを経由せずWebブラウザから直接行う。

(iv) PCのスタブリゾルバは，社内DNSサーバで名前解決を行う。

(v) PC，サーバセグメントとDMZのサーバでは，マルウェア対策ソフトが稼働している。マルウェア定義ファイルの更新は，プロキシサーバ経由で行う。

(vi) (b)PCには，L3SWで稼働するDHCPサーバから，PCのIPアドレス，サブネットマスク及びその他のネットワーク情報が付与される。

図1中のFWに設定されている通信を許可するルールを表1に示す。

表1　FWに設定されている通信を許可するルール

項番	アクセス経路	送信元	宛先	プロトコル／ポート番号
1	インターネット→DMZ	any	ア	TCP/53，イ
2		any	ウ	TCP/443
3	DMZ→インターネット	ア	any	TCP/53，イ
4		エ	オ	TCP/80，TCP/443
5	内部LAN→DMZ	カ	ア	TCP/53，イ
6		サーバセグメント	プロキシサーバ	TCP/8080 [1)]
7		PCセグメント	プロキシサーバ	TCP/8080 [1)]

注記　FWは，ステートフルパケットインスペクション機能をもつ。
注[1)]　TCP/8080は，代替HTTPのポートである。

次に，X主任は，アカウント情報の一元管理をDSによって行い，DSの情報を利用してSSOを実現させることを考え，ケルベロス認証によるSSOについて検討した。

〔ケルベロス認証の概要と通信手順〕

X主任が調査して理解した，ケルベロス認証の概要と通信手順を次に示す。

・ケルベロス認証では，共通鍵暗号による認証及びデータの暗号化を行っている。

・PCとサーバの鍵の管理及びチケットの発行を行う鍵配布センタ（以下，KDCという）が，DSから取得したアカウント情報を基にPC又はサーバの認証を行う。

・KDCが管理するドメインに所属するPCとサーバの鍵は，事前に生成してPC又はサーバに登録するとともに，全てのPCとサーバの鍵をKDCにも登録しておく。

・チケットには，PCの利用者の身分証明書に相当するチケット（以下，TGTという）と，PCの利用者がサーバでの認証を受けるためのチケット（以下，STという）の2種類があり，これらのチケットを利用してSSOが実現できる。

・PCの電源投入後に，利用者がID，パスワード（以下，PWという）を入力してKDCでケルベロス認証を受けると，HTTP over TLSでアクセスする業務サーバや営業支援サーバにも，ケルベロス認証向けのAPIを利用すればSSOが実現できる。

・KDCは，導入予定のDSで稼働する。

X主任は，内部LANにDSを導入したときの，SSOの動作をまとめた。PCの起動から営業支援サーバアクセスまでの通信手順を図2に示す。

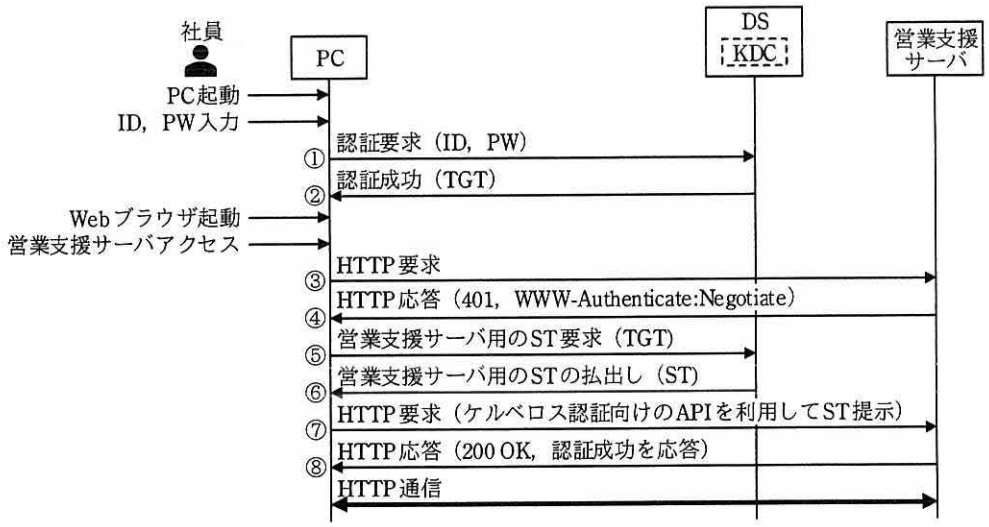


図2　PCの起動から営業支援サーバアクセスまでの通信手順（抜粋）

図2中の，①～⑧の動作の概要を次に示す。

① PC は，DS で稼働する KDC に ID，PW を提示して，認証を要求する。

② KDC は，ID，PW が正しい場合に TGT を発行し，PC の鍵で暗号化した TGT を PC に払い出す。PC は，TGT を保管する。

③ 省略

④ 省略

⑤ PC は，KDC に TGT を提示して，営業支援サーバのアクセスに必要な ST の発行を要求する。

⑥ KDC は，TGT を基に，PC の身元情報，セッション鍵などが含まれた ST を発行し，営業支援サーバの鍵で ST を暗号化する。さらに，KDC は，暗号化した ST にセッション鍵などを付加し，全体を PC の鍵で暗号化した情報を PC に払い出す。セッション鍵は，通信相手の正当性の検証などに利用される。

⑦ PC は，全体が暗号化された情報の中から ST を取り出し，ケルベロス認証向けの API を利用して，ST を営業支援サーバに提示する。

⑧ 営業支援サーバは，ST の内容を基に PC を認証するとともに，アクセス権限を PC に付与して，HTTP 応答を行う。

TGT と ST には，有効期限が設定されている。(c) PC とサーバ間で，有効期限が正しく判断できていない場合は，有効期限内でも，PC が提示した ST を，サーバが使用不可と判断する可能性があるので，PC とサーバでの対応が必要である。

〔SRV レコードの働きと設定内容〕

次に，X 主任は，ケルベロス認証を導入するときのネットワーク構成について検討した。ケルベロス認証導入時には，DNS のリソースレコードの一つである SRV レコードの利用が推奨されているので，SRV レコードについて調査した。

DNS サーバに SRV レコードが登録されていれば，サービス名を問い合わせることによって，当該サービスが稼働するホスト名などの情報が取得できる。

SRV レコードのフォーマットを図 3 に示す。

_Service._Proto.Name	TTL	Class	SRV	Priority	Weight	Port	Target

図3　SRV レコードのフォーマット

X 主任は，図 1 に示したように，内部 LAN に DS を 2 台導入して冗長化し，それぞれの DS でケルベロス認証を稼働させる構成を考えた。

図 3 中の，Service には，ケルベロス認証のサービス名である，kerberos を記述する。Priority は，同一サービスの SRV レコードが複数登録されている場合に，利用する SRV レコードを判別するための優先度を示す。Priority が同じ値の場合は，Weight で Target に記述するホストの使用比率を設定する。Port には，サービスを利用するときのポート番号を記述する。

X 主任は，2 台の DS でケルベロス認証を稼働させる場合の，SRV レコードの設定内容を検討した。

X 主任が作成した，ケルベロス認証向けの SRV レコードの内容を図 4 に示す。ここで，DS1 と DS2 は，本社に導入予定の DS のホスト名である。

_Service._Proto.Name	TTL	Class	SRV	Priority	Weight	Port	Target
_kerberos._tcp.naibulan.y-sha.jp.	43200	IN	SRV	120	2	88	DS1.naibulan.y-sha.jp.
_kerberos._tcp.naibulan.y-sha.jp.	43200	IN	SRV	120	1	88	DS2.naibulan.y-sha.jp.

図4　ケルベロス認証向けの SRV レコードの内容

X 主任は，調査・検討結果を基に SSO の導入構成案をまとめ，Z 課長に提出した。導入構成案が承認され，実施に移されることになった。

設問 1　〔ネットワーク構成及び機器の設定と利用形態〕について，(1)～(4) に答えよ。

(1) 本文中の下線 (a) の動作を行うために，PC のプロキシ設定で登録すべき内容について，40 字以内で述べよ。

(2) 本文中の下線 (b) について，(iii)～(v) の実行を可能とするための，その他のネットワーク情報を二つ答えよ。

(3) 表 1 中の［ア］，［ウ］～［カ］に入れる字句を，図 1 又は表 1 中の字句を用いて答えよ。

(4) 表1中の［　イ　］に入れるプロトコル／ポート番号を答えよ。

設問2　〔ケルベロス認証の概要と通信手順〕について，(1)～(3)に答えよ。

(1) 攻撃者が図2中の②の通信を盗聴して通信データを取得しても，攻撃者は，⑦の通信を正しく行えないので，営業支援サーバを利用することはできない。⑦の通信を正しく行えない理由を，15字以内で述べよ。

(2) 図2中で，ケルベロス認証サービスのポート番号88が用いられる通信を，①～⑧の中から全て選び記号で答えよ。

(3) 本文中の下線(c)の問題を発生させないための，PCとサーバにおける対応策を，20字以内で述べよ。

設問3　〔SRVレコードの働きと設定内容〕について，(1)～(3)に答えよ。

(1) ケルベロス認証を行うPCが，図4のSRVレコードを利用しない場合，PCに設定しなければならないサーバに関する情報を，25字以内で答えよ。

(2) 図4のSRVレコードが，PCのキャッシュに存在する時間は何分かを答えよ。

(3) 図4の二つのSRVレコードの代わりに，図5の一つのSRVレコードを使った場合，DS1とDS2の負荷分散はDNSラウンドロビンで行わせることになる。図4と同様の比率でDS1とDS2が使用されるようにする場合の，Aレコードの設定内容を，50字以内で述べよ。ここで，DS1のIPアドレスをadd1，DS2のIPアドレスをadd2とする。

_Service._Proto.Name	TTL	Class	SRV	Priority	Weight	Port	Target
_kerberos._tcp.naibulan.y-sha.jp.	43200	IN	SRV	120	1	88	DS.naibulan.y-sha.jp.

図5　変更後のSRVレコードの内容

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。