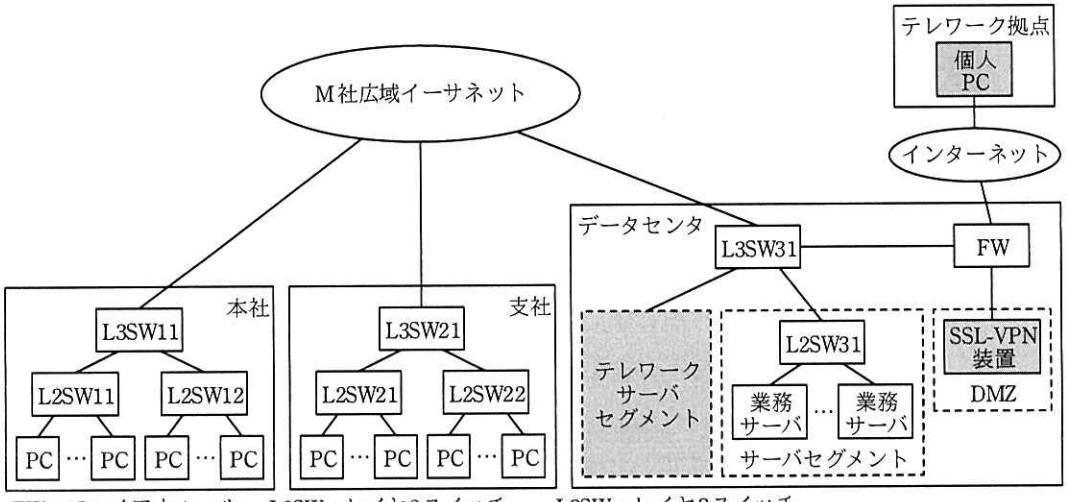
問1　テレワーク環境の導入に関する次の記述を読んで，設問1～5に答えよ。

K社は，東京に本社を構える中堅の製造業者である。東京の本社のほかに，大阪の支社，及び関東圏内のデータセンタがある。このたびK社では，テレワーク環境を導入し，K社社員が自宅などをテレワーク拠点として，個人所有のPC（以下，個人PCという）を利用して業務を行う方針を立てた。また，業務の重要性から，ネットワークの冗長化を行うことにした。これらの要件に対応するために，情報システム部のP主任が任命された。K社の現行のネットワーク及び導入予定の機器を図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
広域イーサネット：広域イーサネットサービス網　業務サーバ：業務アプリケーションサーバ
テレワークサーバセグメント：テレワークのための機器で構成するセグメント
注記　網掛け部分は，テレワーク環境として導入予定の機器を示す。

図1　K社の現行のネットワーク及び導入予定の機器（抜粋）

〔現行のネットワーク構成〕

図1の概要を次に示す。

・本社，支社，データセンタはM社の広域イーサネットで接続されている。
・サーバセグメントに設置された業務サーバに，社内のPCからアクセスして各種業務を行っている。
・FWは，社内からインターネットへのアクセスのためにアドレス変換（NAPT）を行っている。

・FW で DMZ を構成し，DMZ にはグローバル IP アドレスが割り当てられている。
・DMZ 以外の社内の全てのセグメントは，プライベート IP アドレスが割り当てられている。
・経路制御の方式は，OSPF が用いられている。
・本社のネットワークアドレスには，172.16.1.0/24 を割り当てている。
・支社のネットワークアドレスには，172.16.2.0/24 を割り当てている。
・データセンタのネットワークアドレスには，172.17.0.0/16 を割り当てている。

〔テレワーク環境導入方針〕

P 主任は，テレワーク環境構築に当たって，導入方針を次のように定め，技術検討を進めることにした。

・テレワーク拠点の個人 PC には業務上のデータを一切置かない運用とするために，仮想デスクトップ基盤（以下，VDI という）の技術を採用する。
・データセンタのテレワークサーバセグメントに VDI サーバを導入する。VDI サーバでは，個人ごとの仮想化された PC（以下，仮想 PC という）を稼働させ，個人 PC から遠隔で仮想 PC を利用可能にする。
・個人 PC には，仮想 PC の画面を操作するソフトウェア（以下，VDI クライアントという）を導入する。
・仮想 PC から，業務サーバへアクセスして業務を行う。社内の PC からは直接業務サーバへアクセスできるので，社内の PC から仮想 PC は利用しない。
・DMZ に SSL-VPN 装置を導入して，テレワーク拠点の個人 PC からデータセンタのテレワークサーバセグメントへのアクセスを実現する。
・情報セキュリティの観点から，SSL-VPN アクセスのための認証は，個人ごとに事前に発行したクライアント証明書を用いて行う。
・SSL-VPN 装置は，個人 PC からの接続時の認証に応じて適切な仮想 PC を特定する。そして，個人 PC からその仮想 PC への VDI の通信を中継する。このような機能をもつ SSL-VPN 装置を選定する。
・テレワークを行う利用者は最大 200 人とする。

〔SSL-VPN 技術調査とテレワーク環境への適用〕

P 主任は，テレワーク拠点からインターネットを介した社内へのアクセスを想定し

て，SSL-VPN の技術について調査を行い，結果を次のようにまとめた。

・SSL-VPN は，TLS プロトコルを利用した VPN 技術である。

・TLS プロトコルは，HTTPS（HTTP over TLS）通信で用いられる暗号化プロトコルであり，インターネットのような公開ネットワーク上などで安全な通信を可能にする。

・TLS プロトコルのセキュリティ機能は，暗号化，通信相手の認証，及び［　ア　］である。

・SSL-VPN は，リバースプロキシ方式，ポートフォワーディング方式，［　イ　］方式の 3 方式がある。

・リバースプロキシ方式の SSL-VPN は，インターネットからアクセスできない社内の Web アプリケーションへのアクセスを可能にする。

・ポートフォワーディング方式の SSL-VPN は，社内のノードに対して TCP 又は UDP の任意の［　ウ　］へのアクセスを可能にする。

・［　イ　］方式の SSL-VPN は，動的にポート番号が変わるアプリケーションプログラムでも社内のノードへのアクセスを可能にする。

・リバースプロキシ方式以外の SSL-VPN を利用するためには，SSL-VPN 接続を開始するテレワーク拠点の PC に，SSL-VPN 接続を行うためのクライアントソフトウェアモジュール（以下，SSL-VPN クライアントという）が必要である。

・TLS プロトコルは，複数のバージョンが存在するが，TLS1.3 は TLS1.2 よりも安全性が高められている。一例を挙げると，TLS1.3 では AEAD（Authenticated Encryption with Associated Data）暗号利用モードの利用が必須となっており，①セキュリティに関する二つの処理が同時に行われる。

・TLS プロトコルで用いられる電子証明書の形式は，X.509 によって定められている。

・認証局（以下，CA という）によって発行された電子証明書には，②証明対象を識別する情報，有効期限，［　エ　］鍵，シリアル番号，CA のデジタル署名といった情報が含まれる。

P 主任は，SSL-VPN の技術調査結果を踏まえ，テレワーク環境への適用を次のとおり定めた。

・SSL-VPN クライアント，クライアント証明書，及び VDI クライアントを，あらか

じめ個人 PC に導入する。

・SSL-VPN 装置へのアクセスポートは，TCP の 443 番ポートとする。

・SSL-VPN 装置で利用する TLS プロトコルのバージョンは，TLS1.3 を用い，それ以外のバージョンが使われないようにする。

・仮想 PC へのアクセスのプロトコルは RDP とし，TCP の 3389 番ポートを利用する。

・SSL-VPN 装置が RDP だけで利用されることを踏まえ，SSL-VPN の接続方式は［ オ ］方式とする。

〔SSL-VPN クライアント認証方式の検討〕

P 主任は，個人 PC から SSL-VPN 装置に接続する際のクライアント認証の利用について整理した。

・個人 PC から SSL-VPN 装置に接続を行う時に利用者のクライアント証明書が SSL-VPN 装置に送られ，③SSL-VPN 装置はクライアント証明書を基にして接続元の身元特定を行う。K 社においては，社員番号を利用者 ID としてクライアント証明書に含めることにする。

・TLS プロトコルのネゴシエーション中に，④クライアント証明書が SSL-VPN 装置に送信され，SSL-VPN 装置で検証される。

・⑤SSL-VPN 装置からサーバ証明書が個人 PC に送られ，個人 PC で検証される。

TLS プロトコルにおける鍵交換の方式には，クライアント側でランダムなプリマスタシークレットを生成して，サーバの RSA［ エ ］鍵で暗号化してサーバに送付することで共通鍵の共有を実現する，RSA 鍵交換方式がある。また，Diffie-Hellman アルゴリズムを利用する鍵交換方式で，DH 公開鍵を静的に用いる方式もある。これらの方式は，⑥秘密鍵が漏えいしてしまったときに不正に復号されてしまう通信のデータの範囲が大きいという問題があり，TLS1.3 以降では利用できなくなっている。TLS1.3 で規定されている鍵交換方式は，［ カ ］，ECDHE，PSK の 3 方式である。

さらに P 主任は，クライアント証明書の発行に関して次のように検討した。

・クライアント証明書の発行に必要な CA を自社で構築して運用するのは手間が掛か

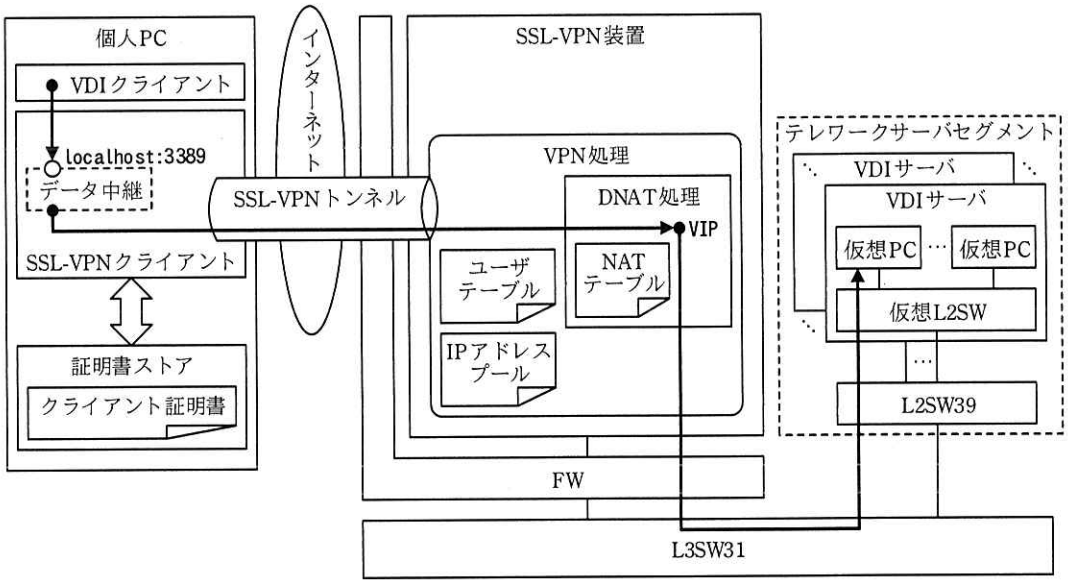
るので，セキュリティ会社である S 社が SaaS として提供する第三者認証局サービス（以下，CA サービスという）を利用する。

・新しいクライアント証明書が必要なときは，利用者の公開鍵と秘密鍵を生成し，公開鍵から証明書署名要求（CSR）を作成して，CA サービスへ提出する。CA サービスは，クライアント証明書を発行してよいかどうかを K 社の管理者に確認するとともに，⑦CSR の署名を検証して，クライアント証明書を発行する。

・クライアント証明書の失効が必要なときは，S 社の CA サービスによって証明書失効手続を行うことによって，CA の証明書失効リストが更新される。証明書失効リストは，失効した日時と⑧クライアント証明書を一意に示す情報のリストになっている。

〔テレワーク環境構成の検討〕

P 主任は，ネットワーク構築ベンダ Q 社の担当者に相談して，Q 社の製品を利用したテレワーク環境の構成を検討した。P 主任が考えたテレワーク環境を図 2 に示す。また，図 2 の主要な構成要素の説明を表 1 に示す。



VIP：仮想IPアドレス　　DNAT：Destination NAT
注記 1　localhost:3389 は，localhost の TCP の 3389 番待受けポートを示す。
注記 2　●→ は，パケットの送信元と宛先を示す。
注記 3　○ は，待受けポートを示す。

図 2　P 主任が考えたテレワーク環境

表1　図2の主要な構成要素

名称	説明
仮想 PC	利用者の業務で利用するための仮想化された PC である。利用者ごとに仮想 PC があらかじめ割り当てられており，IP アドレスは静的に割り当てられている。それぞれの仮想 PC は RDP 接続を TCP の 3389 番ポートで待ち受けている。
VDI サーバ	仮想 PC を稼働させるためのサーバである。複数の VDI サーバで，全利用者分の仮想 PC を収容する。システム立上げ時に全仮想 PC が起動される。 VDI サーバ内の仮想 PC は仮想 L2SW に接続される。仮想 L2SW は VDI サーバの物理インタフェースを通じて L2SW39 に接続される。
L2SW39	複数の VDI サーバを収容する L2SW である。
SSL-VPN 装置	SSL-VPN 接続要求を受けて SSL-VPN トンネルの処理を行い，仮想 PC へ RDP 接続を中継する。この一連の処理を VPN 処理という。VPN 処理はユーザテーブルと NAT テーブルの二つのテーブルを利用する。DNAT 処理のための仮想的な宛先 IP アドレスである VIP が設定される。
VDI クライアント	個人 PC で，仮想 PC の画面を操作するクライアントソフトウェア
SSL-VPN クライアント	SSL-VPN を利用するために個人 PC にインストールされたソフトウェアモジュールである。証明書ストアに格納されたクライアント証明書を用いて処理を行う。VDI クライアントから localhost の TCP の 3389 番ポートへの接続を受け付け，SSL-VPN 装置にその通信を中継する。

SSL-VPN 装置の⑨ユーザテーブルは，SSL-VPN 接続時の処理に必要な情報が含まれるテーブルであり，仮想 PC の起動時に自動設定される。

SSL-VPN 装置の NAT テーブルは，SSL-VPN クライアントからの通信を適切な仮想 PC に振り向けるためのテーブルである。SSL-VPN 装置が SSL-VPN トンネルから VIP 宛てのパケットを受けると，適切な仮想 PC の IP アドレスに DNAT 処理して送る。この処理のために NAT テーブルがあり，SSL-VPN で認証処理中にエントリが作成される。

IP アドレスプールは，SSL-VPN クライアントに付与する IP アドレスのためのアドレスプールであり，172.16.3.1～172.16.3.254 を設定する。

P 主任が考えた，図 2 のテレワーク環境の VDI クライアントから仮想 PC までの接続シーケンスを図 3 に示す。

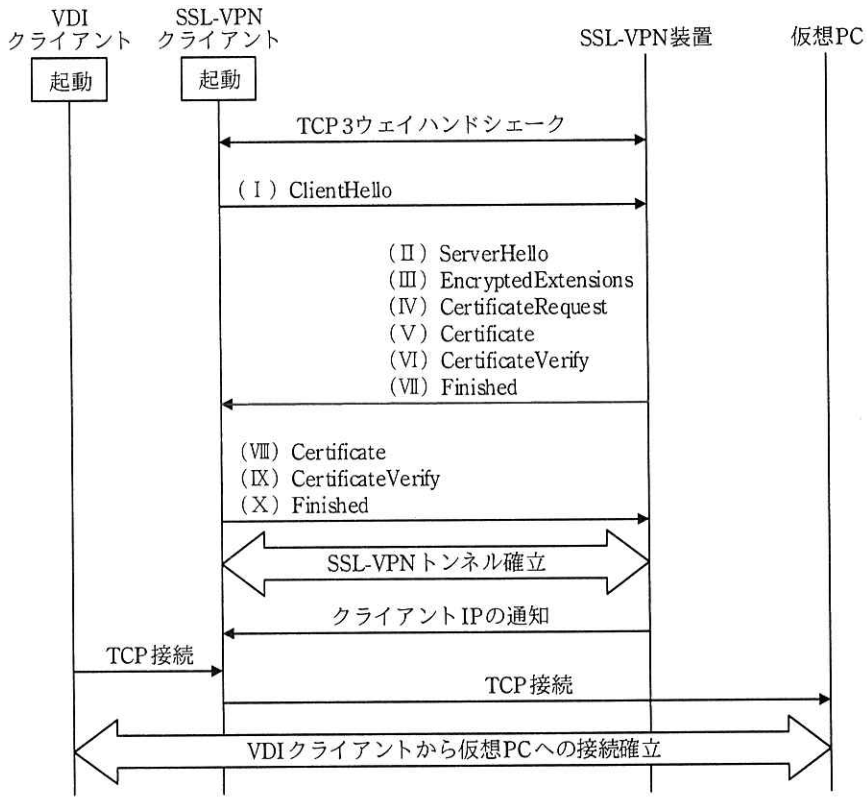


図 3　VDI クライアントから仮想 PC までの接続シーケンス（抜粋）

図 3 の動作の概要を次に示す。

(1) 個人 PC で SSL-VPN クライアントと VDI クライアントを起動する。

(2) SSL-VPN クライアントは，SSL-VPN 装置に対するアクセスを開始する。

(3) SSL-VPN 装置は，クライアント証明書による認証を行う。

(4) SSL-VPN クライアントと SSL-VPN 装置間に，TLS セッションが確立される。この TLS セッションは SSL-VPN トンネルとして利用する。

(5) SSL-VPN 装置は，SSL-VPN クライアントに割り当てる IP アドレスを管理するための IP アドレスプールから IP アドレスを割り当て，SSL-VPN クライアントに通知する。この割り当てられた IP アドレスを，クライアント IP という。

(6) SSL-VPN 装置は，⑩ユーザテーブルを検索して得られる IP アドレスを用いて，NAT テーブルのエントリを作成する。

(7) SSL-VPN クライアントは，localhost:3389 の待ち受けを開始する。

(8) VDI クライアントは，localhost:3389 へ TCP 接続を行う。

(9) SSL-VPN クライアントは，SSL-VPN トンネルを通じて，VIP の 3389 番ポートへ向けての TCP 接続を開始する。

(10) SSL-VPN 装置は，VIP に届いた一連のパケットを DNAT 処理して仮想 PC に転送する。これによって，SSL-VPN クライアントと仮想 PC の間に TCP 接続が確立する（以下，この接続をリモート接続という）。

(11) SSL-VPN クライアントは，localhost:3389 とリモート接続の間のデータ中継を行う。

上記の (1)〜(11) によって，VDI クライアントから仮想 PC までの接続が確立し，個人 PC から仮想 PC のデスクトップ環境が利用可能になる。

〔ネットワーク冗長化の検討〕

次に P 主任は，次のようにネットワークの冗長化を考えた。P 主任が考えた新たな冗長化構成を図 4 に示す。

・PC と業務サーバの間のネットワーク機器のうち，PC を収容する L2SW 以外の機器障害時に，PC から業務サーバの利用に影響がないようにする。

・拠点間接続の冗長化のために，新たに N 社の広域イーサネットを契約する。その回線速度と接続トポロジは現行の M 社広域イーサネットと同等とする。

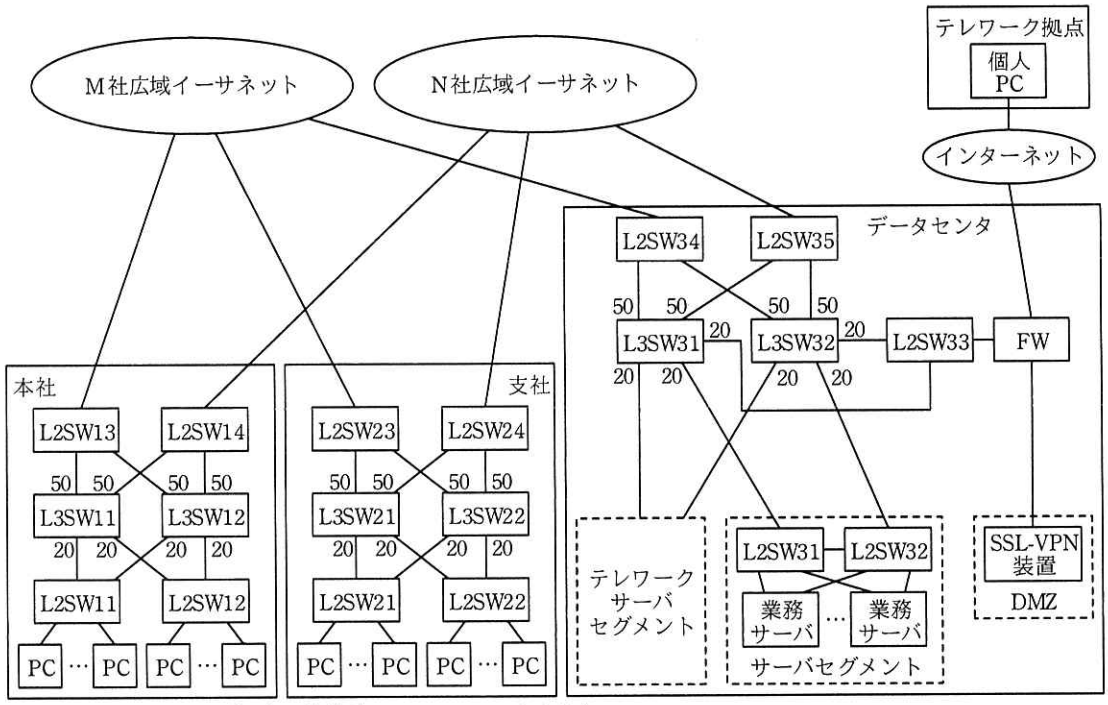
・通常は，M 社と N 社の広域イーサネットの両方を利用する。

・本社に L2SW13，L2SW14，L3SW12，支社に L2SW23，L2SW24，L3SW22，データセンタに L2SW32〜L2SW35，L3SW32 を新たに導入する。

・業務サーバの NIC はチーミングを行う。

・サーバセグメントに接続されている L3SW は VRRP によって冗長化を行う。

・ネットワーク全体の経路制御はこれまでどおり，OSPF を利用し，OSPF エリアは全体でエリア 0 とする。



注記　図中の L3SW のポートの数値は，OSPF のコストを示す。

図 4　P 主任が考えた新たな冗長化構成（抜粋）

全ての L3SW で OSPF を動作させ，冗長経路の OSPF のコストを適切に設定することによって，⑪ OSPF の Equal Cost Multi-path 機能（以下，ECMP という）が利用できると考え，図 4 に示すコスト設定を行うことにした。その場合，例えば⑫ L3SW11 のルーティングテーブル上には，サーバセグメントへの同一コストの複数の経路が確認できる。

K 社で利用している L3SW のベンダに ECMP の経路選択の仕様を問い合わせたところ，次の仕様であることが分かった。

・最大で四つの同一コストルートまでサポートする。
・動作モードとして，パケットモードとフローモードがある。
・パケットモードの場合，パケットごとにランダムに経路を選択し，フローモードの場合は，送信元 IP アドレスと宛先 IP アドレスからハッシュ値を計算して経路選択を行う。

P 主任は，K 社の社内の PC と業務サーバ間の通信における⑬通信品質への影響を考慮して，フローモードを選択することにした。また，フローモードでも⑭複数回

線の利用率がほぼ均等になると判断した。

次に，P 主任は，サーバセグメントに接続されている L3SW の冗長化について，図5のように行うことにした。

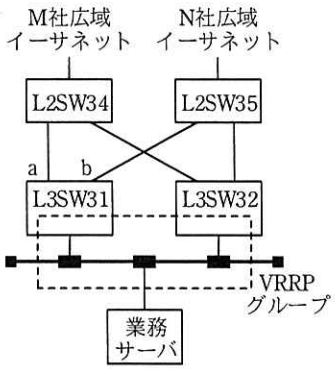


図5　サーバセグメントに接続されている L3SW の冗長化

図5において，L3SW31 と L3SW32 で VRRP を構成し，L3SW31 が VRRP マスタとなるように優先度を設定する。また，L3SW31 において，⑮図5中の a 又は b での障害をトラッキングするように VRRP の設定を行う。これによって，a 又は b のインタフェースでリンク障害が発生した場合でも，業務サーバから PC へのトラフィックの分散が損なわれないと考えた。

P 主任は，以上の技術項目の検討結果について情報システム部長に報告し，SSL-VPN 導入，N 社と S 社サービス利用及びネットワーク冗長化について承認された。

設問1　本文中の［　ア　］～［　カ　］に入れる適切な字句を答えよ。

設問2　〔SSL-VPN 技術調査とテレワーク環境への適用〕について，(1)，(2) に答えよ。

(1) 本文中の下線①について，同時に行われる二つのセキュリティ処理を答えよ。

(2) 本文中の下線②について，電子証明書において識別用情報を示すフィールドは何か。フィールド名を答えよ。

設問3　〔SSL-VPN クライアント認証方式の検討〕について，(1)～(6) に答えよ。

(1) 本文中の下線③について，クライアント証明書で送信元の身元を一意に特

定できる理由を，“秘密鍵”という用語を用いて 40 字以内で述べよ。

(2) 本文中の下線④について，クライアント証明書の検証のために，あらかじめ SSL-VPN 装置にインストールしておくべき情報を答えよ。

(3) 本文中の下線⑤について，検証によって低減できるリスクを，35 字以内で答えよ。

(4) 本文中の下線⑥について，TLS1.3 で規定されている鍵交換方式に比べて，広く復号されてしまう通信の範囲に含まれるデータは何か。“秘密鍵”と“漏えい”という用語を用いて，25 字以内で答えよ。

(5) 本文中の下線⑦について，利用者が CA サービスに CSR を提出するときに署名に用いる鍵は何か。また，CA サービスが CSR の署名の検証に用いる鍵は何か。本文中の用語を用いてそれぞれ答えよ。

(6) 本文中の下線⑧について，証明書失効リストに含まれる，証明書を一意に識別することができる情報は何か。その名称を答えよ。

設問 4 〔テレワーク環境構成の検討〕について，(1)，(2) に答えよ。

(1) 本文中の下線⑨について，ユーザテーブルに含まれる情報を 40 字以内で答えよ。

(2) 本文中の下線⑩について，検索のキーとなる情報はどこから得られるどの情報か。25 字以内で答えよ。また，SSL-VPN 装置は，その情報をどのタイミングで得るか。図 3 中の (I)～(X) の記号で答えよ。

設問 5 〔ネットワーク冗長化の検討〕について，(1)～(5) に答えよ。

(1) 本文中の下線⑪について，P 主任が ECMP の利用を前提にしたコスト設定を行う目的を，30 字以内で答えよ。

(2) 本文中の下線⑫について，経路数とそのコストをそれぞれ答えよ。

(3) 本文中の下線⑬について，フローモードの方が通信品質への影響が少ないと判断した理由を 35 字以内で述べよ。

(4) 本文中の下線⑭について，利用率がほぼ均等になると判断した理由を L3SW の ECMP の経路選択の仕様に照らして，45 字以内で述べよ。

(5) 本文中の下線⑮について，この設定による VRRP の動作を“優先度”という用語を用いて 40 字以内で述べよ。