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。

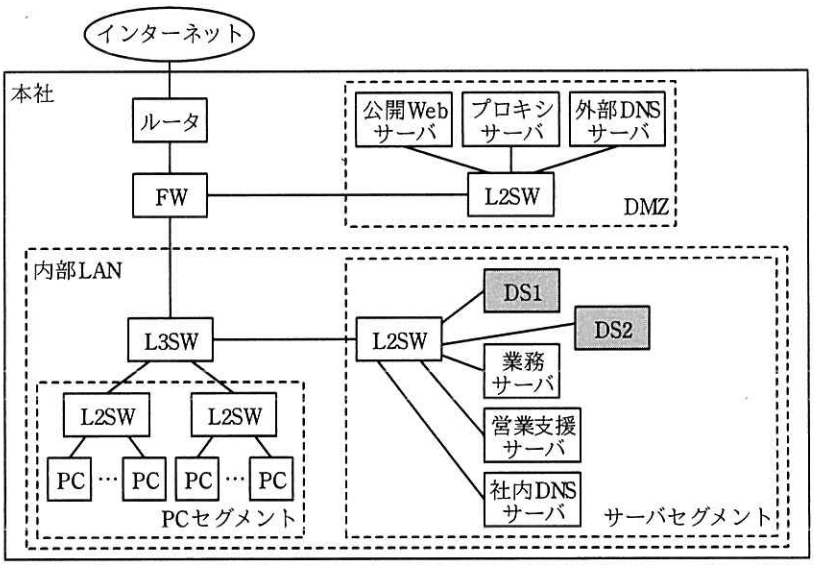
Y社は，医療機器販売会社であり，都内に本社を構えている。受発注業務システムのサーバ（以下，業務サーバという），営業活動支援システムのサーバ（以下，営業支援サーバという）など，複数のサーバを本社で運用している。

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。

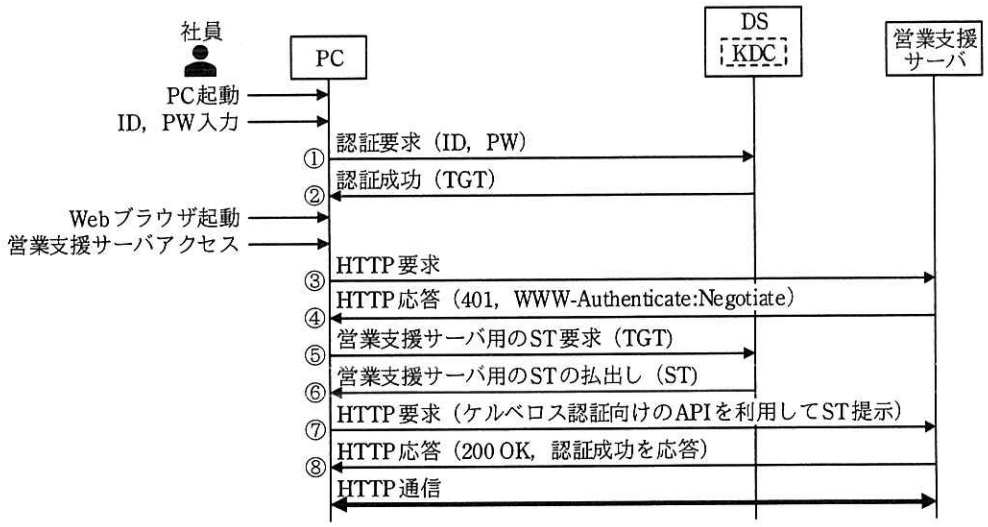


図2　PCの起動から営業支援サーバアクセスまでの通信手順（抜粋）

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