問1　利用者 ID 管理システム及び認証システムの設計に関する次の記述を読んで，設問1～6に答えよ。

N 社は，従業員数 20,000 名の大手金融機関である。N 社はこれまで，日本の顧客企業の海外展開に合わせて海外にも支店を設け，顧客企業の現地法人及びその従業員向けの金融サービスを提供することによって，海外での取引を急速に拡大させてきた。N 社は現在，日本，欧米，アジアという地域ごとに業務を行っており，システムも地域ごとに構築している。N 社の正社員の人事管理も地域ごとに人事システムで行っているが，契約社員は，支店ごとに契約社員を管理する者（以下，管理者という）が人事システムを使わずに管理している。

N 社は，より広い範囲の顧客企業及び個人顧客に世界共通の金融サービスを提供するための第一歩として，各地域の情報系システム（以下，社内システムという）のうち，機能面で共通性の高いものを，全地域から利用できる共通のシステム（以下，G システムという）として一本化し，各地域の社内システムの利用者全員に，G システムと，利用者が所属する地域の社内システムを併用させることにした。また，地域によって異なっている利用者 ID（以下，ID という）管理及び利用者認証の方式と運用を統一し，セキュリティ管理の一元化及び効率向上を実現することにした。N 社の各地域における利用者認証方式の概要を表1に示す。

表1　N 社の各地域における利用者認証方式の概要

種別＼地域	日本	欧米地域	アジア地域
PC における利用者認証	IC カードによる利用者認証（ディレクトリサーバ製品 Q を利用）	ID，パスワードによる利用者認証（ディレクトリサーバ製品 Q を利用）	
社内システムにおける利用者認証	エージェント型の認証サーバを開発して利用	リバースプロキシ型の認証サーバ製品 P を利用	
PC と社内システムにおけるシングルサインオン	SPNEGO プロトコル[1]によって実現		実現されていない

注[1]　RFC 4178 The Simple and Protected Generic Security Service Application Program Interface (GSS-API) Negotiation Mechanism

〔日本における ID 管理・認証の方式〕

日本の N 社では，利用者が日本の PC（以下，日本 PC という）に接続された IC カードリーダに IC カードを差し込むと，IC カードから ID とディジタル証明書（以下，証明書という）が読み取られ，ディレクトリサーバ製品 Q を用いた日本のディレクト

リサーバ（以下，ディレクトリサーバを DS という）において利用者認証が行われる。日本の DS（以下，日本 DS という）は，PC における利用者認証が成功すると，日本 PC に当該利用者のチケット認可チケット（以下，TGT という）を発行する。日本 PC は N 社が一括調達したものであり，IC カードリーダは，日本 PC 専用に開発されたものである。

利用者が日本 PC のブラウザを起動すると，ブラウザは，ホームページとして設定された日本の認証サーバ（以下，日本認証サーバという）にアクセスする。日本認証サーバは，認証していないブラウザからの HTTP 要求に対して，HTTP ステータスコード 401，Negotiate の値をもつ WWW-Authenticate ヘッダ，並びに ID 及びパスワードの入力画面を含む HTTP 応答を返す。そうすると，ブラウザは，日本認証サーバのアクセスに必要なサービスチケット（以下，ST という）の提示，又はフォーム認証による ID とパスワードの入力のどちらかを行う。日本 PC のブラウザは，SPNEGO によるシングルサインオン（以下，SSO という）を利用する設定が行われており，前述の HTTP 応答を受信すると，日本 DS に TGT を提示して ST を受け取り，その ST を日本認証サーバに提示して日本の社内システム（以下，日本社内システムという）における利用者認証が成功する。ST には暗号化された ID が含まれており，ST を受け取ったサーバは，復号処理によって ID を得ることができる。

日本認証サーバは，利用者認証が成功すると，認証 Cookie を発行し，認証成功を示すメッセージと日本のポータルサーバ（以下，日本ポータルという）へのリンクをブラウザに表示する。利用者がそのリンクをクリックすると，日本ポータルは，認証 Cookie の検証を行う。検証が成功すると，当該利用者がアクセス可能な日本社内システムへのリンクが並んだポータル画面をブラウザに表示する。

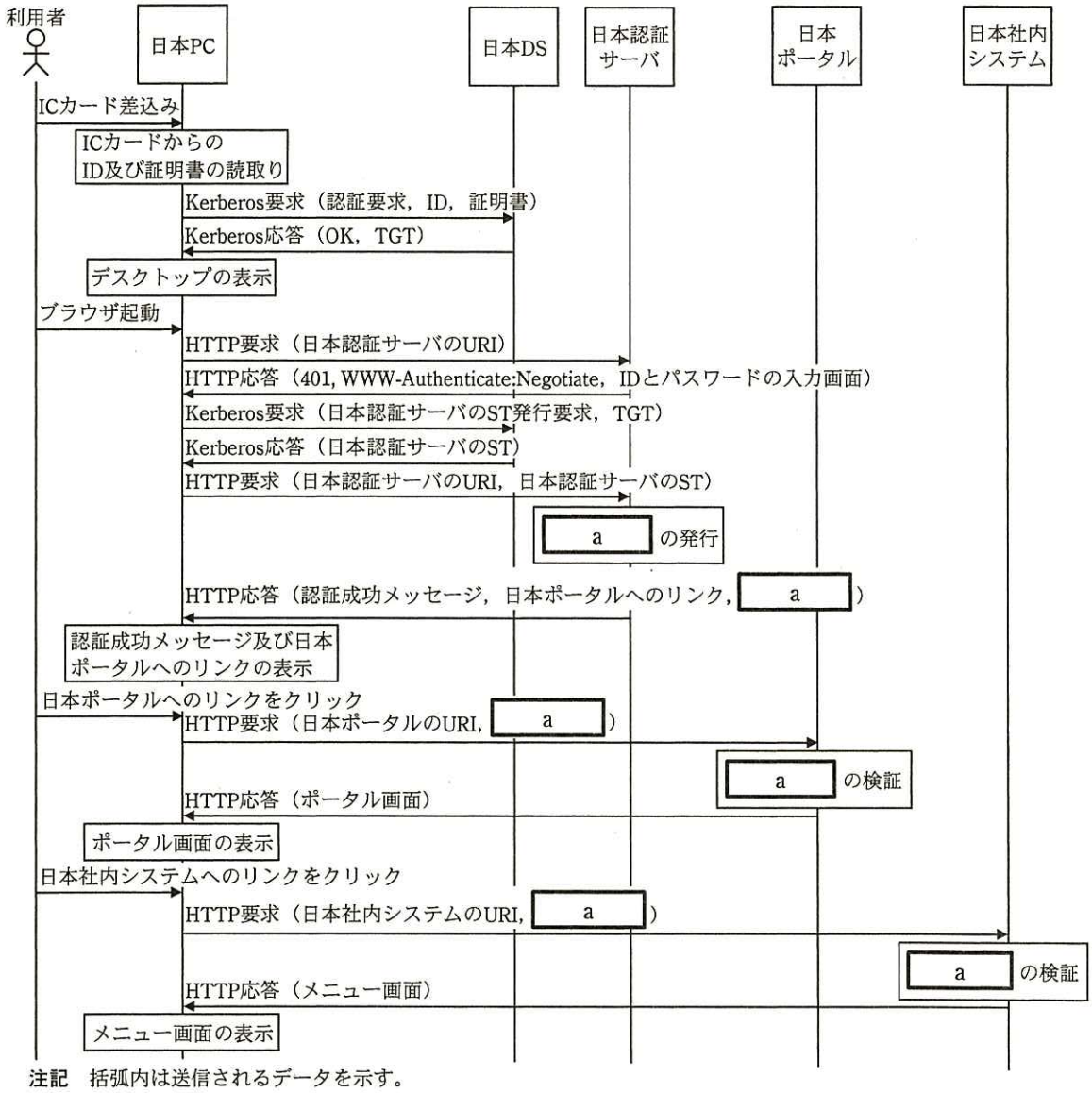
利用者が日本社内システムにアクセスすると，日本社内システムは，認証 Cookie の検証を行った後，メニュー画面をブラウザに表示する。日本ポータル及び日本社内システムでの認証 Cookie の検証では，日本認証サーバと併せて開発された，エージェントと呼ばれる Java プログラムがアプリケーションプログラムからメソッドとして呼び出される。

正社員が入社すると，人事管理手続に基づき，正社員情報の確認と登録の承認が行われた後，人事システムに登録される。人事システムに新しい正社員情報が登録されると，情報システム部は，当該正社員の証明書を発行し，ID と証明書を日本 DS に登録し，ID と証明書を格納した IC カードを当該正社員に貸与する。

契約社員が日本社内システムにアクセスする必要がある場合，管理者が所属長に対して当該契約社員のシステム利用申請を行い，承認を得る。その後，日本の情報システム部は，当該契約社員の証明書を発行し，ID と証明書を日本 DS に登録し，ID と証明書を格納した IC カードを管理者経由で当該契約社員に貸与する。

ID の先頭 2 桁は，正社員では AA，契約社員では本店・支店の識別番号であり，後続 6 桁は，正社員では社員番号，契約社員では管理者が採番した番号である。

日本における利用者認証の通信シーケンスを図 1 に示す。



注記　括弧内は送信されるデータを示す。

図 1　日本における利用者認証の通信シーケンス（概要）

〔欧米地域におけるID管理・認証の方式〕

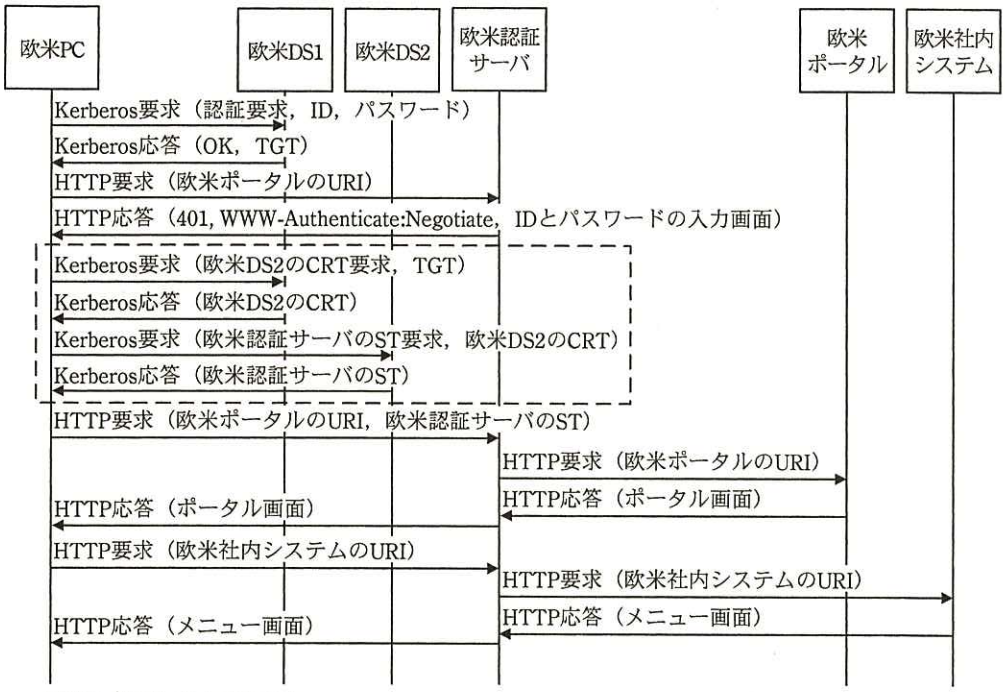
20年前から支店を設けている欧米地域では，N社は，ブラウザ，製品Qを用いた欧米地域のDS1（以下，欧米DS1という）及び欧米地域のDS2（以下，欧米DS2という）並びにリバースプロキシ型の認証サーバ製品Pを用いた欧米地域の認証サーバ（以下，欧米認証サーバという）を組み合わせて，SPNEGOによるSSOを実現している。製品Pは，SPNEGOによるSSOを利用するように設定されると，認証されていないブラウザからのHTTP要求に対して，日本認証サーバと同じ動作をしてSPNEGOによる利用者認証を行う。欧米地域のPC（以下，欧米PCという）のブラウザ及び欧米認証サーバは，SPNEGOによるSSOを利用するように設定されている。

欧米DS1には欧米PCのコンピュータ名及び欧米地域のIDが，欧米DS2には欧米地域の各サーバのコンピュータ名が，それぞれ登録されている。欧米DS1及び欧米DS2には，お互いを信頼するという設定が行われている（以下，信頼関係が結ばれているという）。現在，N社の中のDS間で信頼関係が結ばれているのは，欧米DS1と欧米DS2間だけである。

利用者が，欧米PCにログオンして，ブラウザを立ち上げると，ブラウザは，ホームページとして設定された欧米地域のポータルサーバ（以下，欧米ポータルという）にアクセスしようとする。

欧米地域におけるID管理の手続は，日本と同様である。欧米地域の情報システム部は，新しい正社員又は契約社員のIDと初期パスワードを欧米DS1に登録し，当該正社員又は管理者に通知する。IDの体系は日本と同じであり，日本と重複しているIDがある。

欧米地域における利用者認証の通信シーケンスを図2に示す。



CRT：相互レルムチケット

欧米社内システム：欧米地域の社内システム

注記１　括弧内は送信されるデータを示す。

注記２　破線の枠内の機能が正しく動作するためには，次の二つの条件が必要である。

・欧米DS1及び欧米DS2の間で信頼関係が結ばれていること

・欧米DS1及び欧米DS2がもつドメイン名，登録されているID及びコンピュータ名が重複していないこと

図２　欧米地域における利用者認証の通信シーケンス（概要）

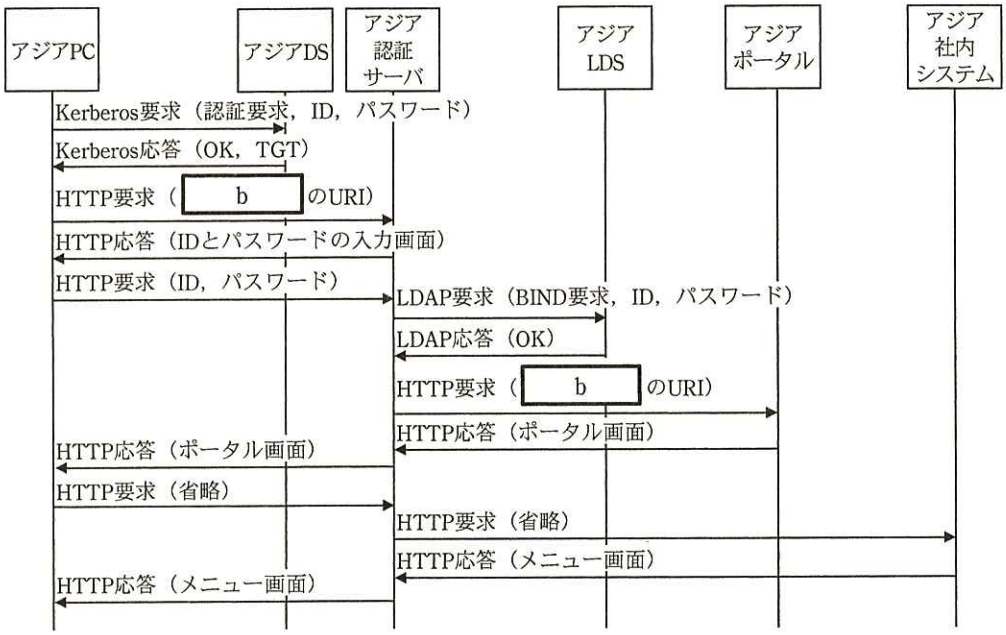
〔アジア地域における ID 管理・認証の方式〕

支店網を急拡大してきたアジア地域において，N 社は，製品 P を用いたアジア地域の認証サーバ（以下，アジア認証サーバという）に，LDAP サーバ製品 R を用いたアジア地域の LDAP サーバ（以下，アジア LDS という）を組み合わせて，SSO を短期間で実現した。ただし，アジア認証サーバは，SPNEGO ではなくフォーム認証を利用しており，アジア地域の PC（以下，アジア PC という）に SPNEGO の設定はされていない。SSO の対象は，アジア地域のポータルサーバ（以下，アジアポータルという）と，アジア地域の社内システム（以下，アジア社内システムという）である。

利用者が，アジア PC にログオンして，ブラウザを立ち上げると，ブラウザは，ホームページとして設定されたアジアポータルにアクセスしようとする。その際，アジア認証サーバは，アジア LDS を参照し，ID とパスワードによる利用者認証を行う。

アジア地域の全ての正社員及び契約社員は，入社時にアジア PC が利用できるように製品 Q を用いたアジア地域の DS（以下，アジア DS という）に ID が登録される。しかし，アジア LDS への ID 登録や削除は人事システムと連携していない。そのため，正社員及び契約社員は，アジア社内システムにアクセスする必要が生じた際に，自ら ID とパスワードの登録をアジア地域の情報システム部に依頼している。情報システム部は，依頼内容に沿ってアジア LDS に ID とパスワードを登録する。他の地域と重複している ID はない。

アジア地域における利用者認証の通信シーケンスを図 3 に示す。



注記　括弧内は送信されるデータを示す。

図 3　アジア地域における利用者認証の通信シーケンス（概要）

〔G システムにおける ID 管理・認証の設計〕

日本の情報システム部の X 部長は，部下の Y さんに，G システムにおける ID 管理，SSO 及びアクセス制御を行うグローバル ID・アクセス管理システム（以下，GIAM システムという）を設計し，情報セキュリティスペシャリストの Z 主任のレビューを受けるように指示した。Y さんは，認証サブシステム，ID 管理サブシステム，ポータルサブシステム（以下，G ポータルという）から成る GIAM システムを設計した。それ

ぞれのサブシステムの概要は次のとおりである。

・認証サブシステム

製品 P を用いた認証サーバ（以下，認証サブシステムの認証サーバを G 認証サーバという）と製品 R を用いた LDAP サーバ（以下，認証サブシステムの LDAP サーバを GLDS という）から成り，G ポータル及び G システムへのアクセスにおいて，N 社全体で一意となる ID（以下，GID という）とパスワードによる利用者認証及び SSO を実現する。利用者認証が成功すると，HTTP ヘッダに GID を埋め込んで G ポータル及び G システムに送信する。

・ID 管理サブシステム

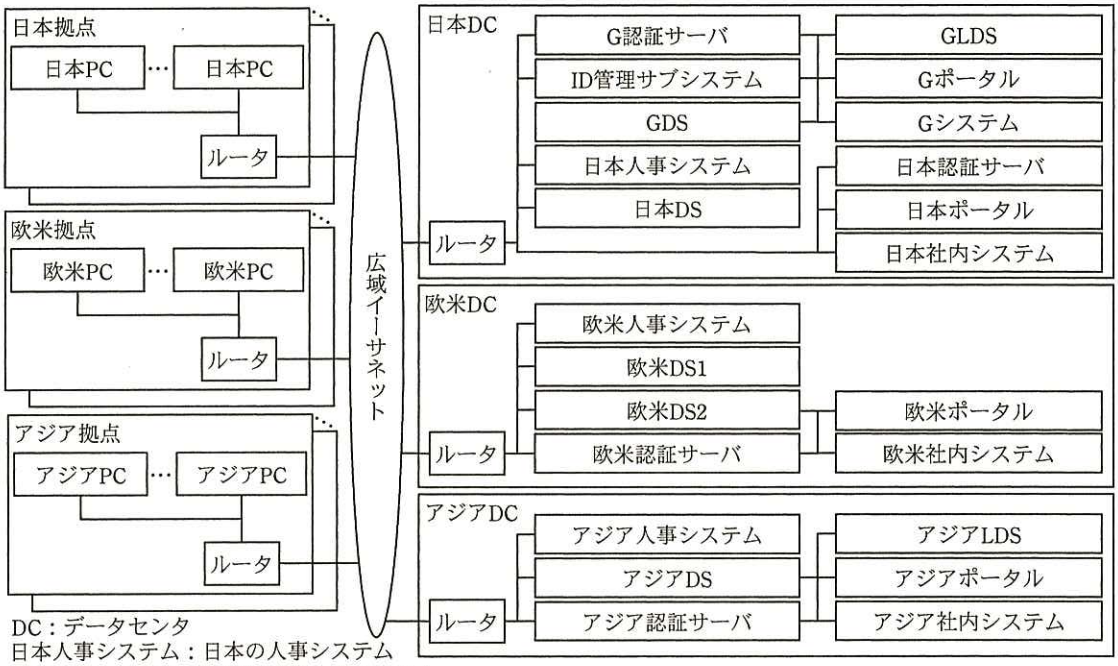
日次で各地域の人事システムから正社員の利用者情報を収集し，新たに登録された正社員に対して，GID と初期パスワードを生成して GLDS に登録する。

・G ポータル

G 認証サーバから渡された GID 及び GLDS に登録された利用者属性に基づいてポータル画面を生成し，G システム及び当該利用者が所属する地域のポータルサーバへのリンクを表示する。全地域の PC ではブラウザに G ポータルをホームページとして設定し，ブラウザが立ち上がると G ポータルのポータル画面が表示されるようにする。

Y さんが設計した，GIAM システム及び関連システムの論理構成を図 4 に，GIAM システムにおける利用者認証の通信シーケンスを図 5 に，それぞれ示す。

なお，図 4 において，グローバル DS（以下，GDS という）には，製品 Q が用いられ，認証サブシステム，ID 管理サブシステム及び G ポータルの各サーバのコンピュータ名が登録される。



DC：データセンタ
日本人事システム：日本の人事システム
欧米人事システム：欧米地域の人事システム
アジア人事システム：アジア地域の人事システム

図４　GIAM システム及び関連システムの論理構成

注記１　括弧内は送信されるデータを示す。
注記２　破線部分については後述する。

図５　GIAM システムにおける利用者認証の通信シーケンス（概要）

Y さんは，GIAM システムの設計について，Z 主任のレビューを受けた。Z 主任は，Y さんに，図 5 中の破線の部分にアジア地域の認証方式を採用した理由を質問した。Y さんは，次の 2 点を説明した。

・①エージェント型の認証サーバを採用した場合，G ポータルや G システムに市販のパッケージ製品を採用する際に大きなカスタマイズが必要となる。

・SPNEGO による SSO を実現するためには，②GDS と各地域の DS に関する変更と③ID 体系に関する変更が必要になり，地域間調整が必要である。

Z 主任は，認証サブシステムの設計を了承した。

次に Z 主任は，④ID 管理サブシステムの設計に不十分な点があることを指摘し，各地域の人事システムとは別のサーバから利用者情報を収集する必要があると助言した。

さらに，Z 主任は，⑤一部の地域で，G ポータルのポータル画面中のリンクから地域のポータルサーバへのアクセスが失敗することを指摘し，G ポータルのポータル画面に載せるリンクを修正する必要があると助言した。

Y さんは Z 主任の助言を反映し，GIAM システムの設計について X 部長の承認を得た。

〔欧米地域からの要望への対応〕

X 部長は，Y さんと Z 主任に対して，GIAM システムの設計内容について，各地域の情報システム部及び利用者の代表者に説明するよう指示した。Y さんと Z 主任が欧米地域に出張して GIAM システムの設計内容を説明したところ，次の要望が挙がった。

要望 1.

現行システムと同様に，一度 PC にログオンすれば，欧米社内システム及び G システムへの SSO ができるようにしてほしい。

要望 2.

ワークスタイル変革及び災害対策として，利用者が自宅から，個人所有の PC やタブレット端末（以下，個人所有機器という）を使って欧米社内システムを利用する方法を検討中である。インターネット経由で社内のシンクライアントサーバにアクセスし，仮想デスクトップから欧米社内システム及び G システムにアクセスする際においても SSO を実現してほしい。ただし，インターネット経由の仮想デスクト

ップへのアクセスにおいては，二要素認証を実装したい。

要望 3.

他地域への出張中でも，仮想デスクトップから，欧米社内システム及び G システムにアクセスする際において SSO を実現してほしい。

Y さんは，GIAM システムに下線②と下線③の変更を行うことにし，欧米地域の三つの要望全てを全地域の利用者に対して実現する拡張 GIAM システムを設計した。

拡張 GIAM システムでは，自宅又は出張先にいる利用者は，個人所有機器から自分が所属する地域の VPN サーバ経由で自分が所属する地域のシンクライアントサーバにアクセスし，G ポータルのポータル画面から，G システム，自分が所属する地域のポータルサーバ及び自分が所属する地域の社内システムにアクセスする。

個人所有機器の業務利用を希望する利用者は，個人所有機器の利用申請を行い，所属長に承認されると，VPN 接続用の ID（以下，VPNID という）とパスワード（以下，VPN パスワードという）が割り当てられ，ハードウェア型のワンタイムパスワード（以下，OTP という）トークンが貸与される。

拡張 GIAM システム及び関連システムの論理構成を図 6 に，個人所有機器からシンクライアントサーバへのアクセスの通信シーケンスを図 7 に，仮想デスクトップから G システムへのアクセスの通信シーケンスを図 8 に，それぞれ示す。

Y さんは，利用者が各地域の PC から G システムにアクセスする場合の通信シーケンスは，図 8 中の仮想デスクトップを各地域の PC に置き換えたものになると考えた。

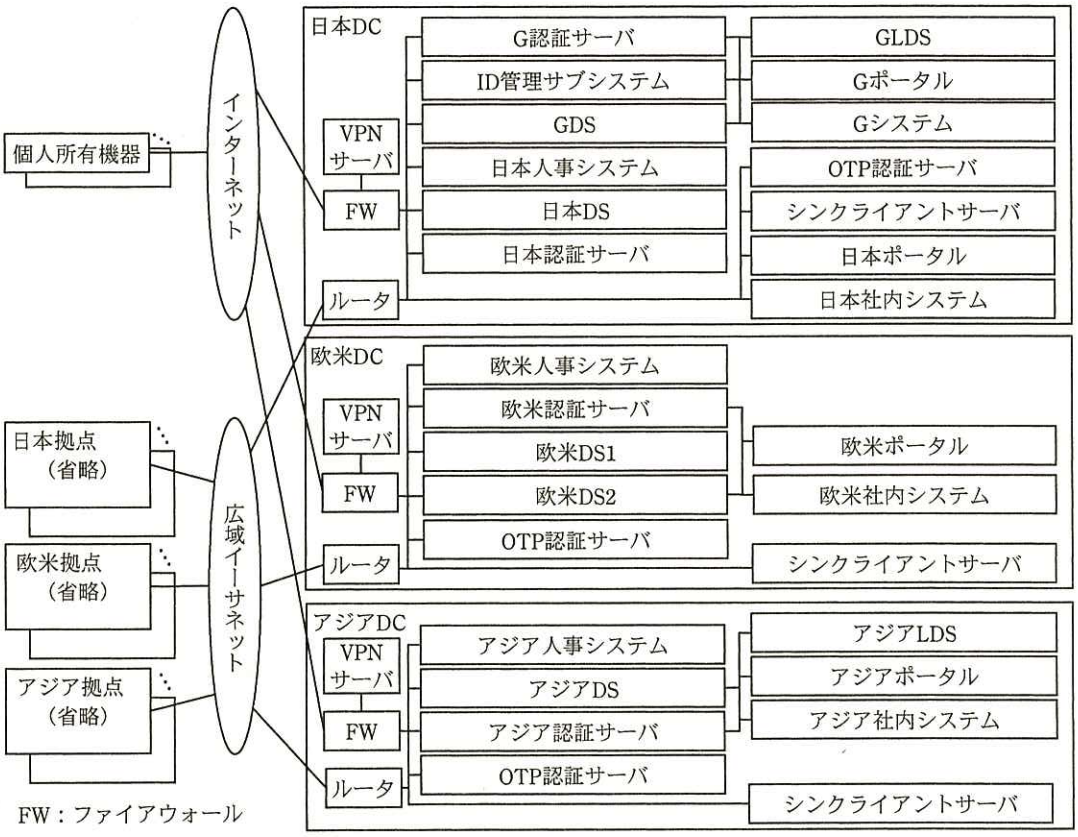
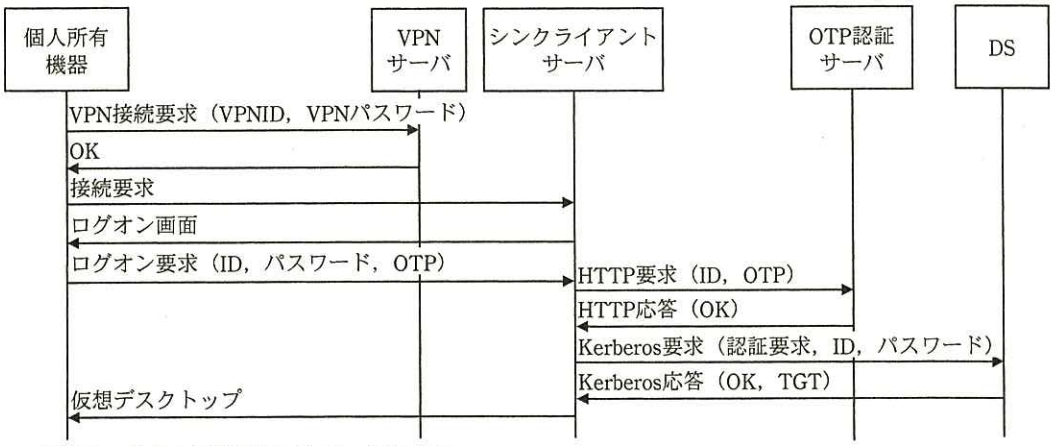
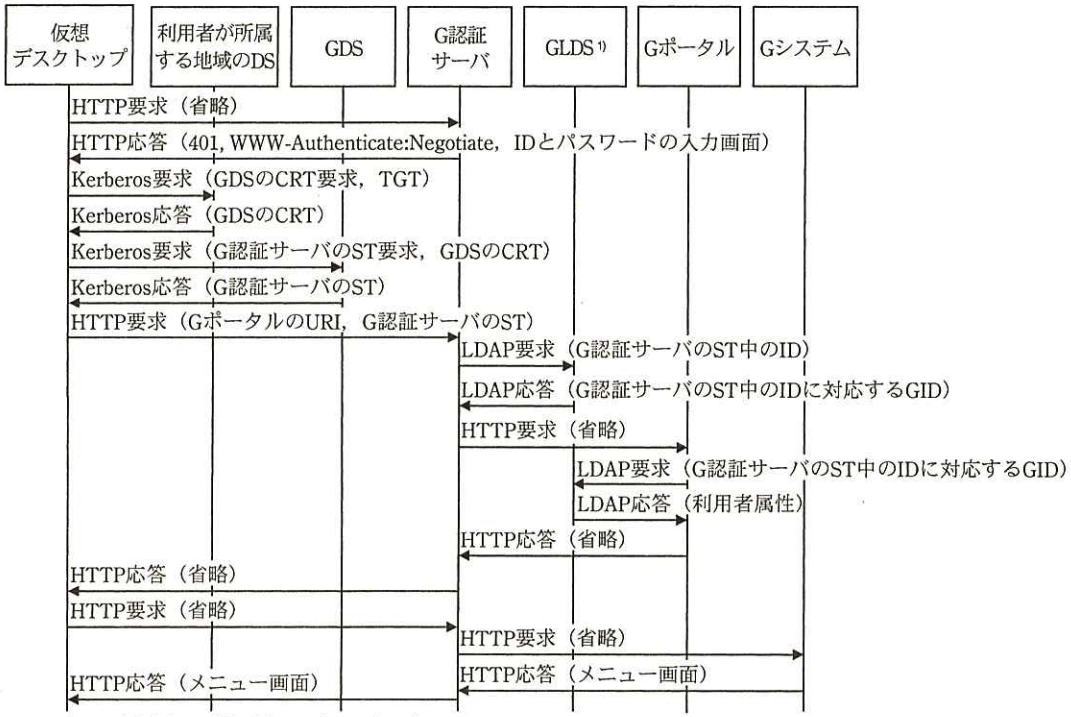


図６　拡張 GIAM システム及び関連システムの論理構成



注記１　括弧内は送信されるデータを示す。
注記２　各サーバは利用者が所属する地域のサーバである。

図７　個人所有機器からシンクライアントサーバへのアクセスの通信シーケンス（概要）



注記　括弧内は送信されるデータを示す。
注1)　GLDSでは，IDとGIDの対応付けをもつ。

図8　仮想デスクトップからGシステムへのアクセスの通信シーケンス（概要）

Y さんは，拡張 GIAM システムの設計について，Z 主任のレビューを受けた。Z 主任は，IC カードによる利用者認証の方式を採用しなかった理由を質問した。⑥Y さんは，採用した場合，IC カードリーダの追加導入や持ち運びが必要になる上，テスト工程の期間と工数が大きくなると説明した。次に，Z 主任は，⑦要望 2 を実現する方法としてシンクライアントサーバを各地域の DC に配置し，利用者が自分の所属する地域のシンクライアントサーバにアクセスするようにした理由を質問した。Y さんは，その理由を説明した。

Z 主任は，⑧一部の地域の利用者は，PC における利用者認証の後，G ポータル及び地域のポータルサーバにアクセスしようとしたときに ID とパスワードの再入力が必要であることを指摘し，当該地域におけるシステム設定の変更が必要であると助言した。

Y さんは，Z 主任の助言を反映し，拡張 GIAM システムの設計について X 部長の承認を得た。Y さんと Z 主任は，再度各地域の情報システム部及び利用者の代表者に説明を行い，合意を得た。各地域の情報システム部は，G システム及び拡張 GIAM システムの構築を始めた。

設問 1　各地域における ID 管理・認証の方式について，(1)～(3)に答えよ。

(1)　図 1 中の [a] に入れる適切な字句を，本文中の用語を用いて答えよ。

(2)　図 3 中の [b] に入れる適切な字句を，図 3 中から選び，答えよ。

(3)　アジア地域におけるアジア LDS への正社員及び契約社員の ID の登録手順について，セキュリティ上の問題点を 45 字以内で述べよ。

設問 2　GIAM システムにおける利用者認証方式について，(1)～(3)に答えよ。

(1)　本文中の下線①について，必要なカスタマイズの内容を 35 字以内で述べよ。

(2)　本文中の下線②について，変更の内容を 25 字以内で述べよ。

(3)　本文中の下線③は，どのような現状の問題を解決するために必要か。30 字以内で述べよ。

設問 3　本文中の下線④について，(1)，(2)に答えよ。

(1)　ID 管理サブシステムの設計における不十分な点を，25 字以内で述べよ。

(2)　利用者情報の収集元として適切なサーバ名を，図 4 中から三つ選び，答えよ。

設問 4　本文中の下線⑤について，地域のポータルサーバへのアクセスが失敗する地域を，本文中の用語を用いて答えよ。また，ポータル画面に載せるリンクはどのサーバの URI にすべきか。サーバ名を 10 字以内で答えよ。

設問 5　〔欧米地域からの要望への対応〕について，(1)～(3)に答えよ。

(1)　拡張 GIAM システムの二要素認証において使われる認証要素を二つ挙げ，それぞれ 8 字以内で答えよ。

(2)　本文中の下線⑥について，Y さんがテスト工程の期間と工数が大きくなると説明したのは，テスト工程でどのような機能検証を行う必要があると考えたからか。25 字以内で述べよ。

(3)　本文中の下線⑦について，利用者が他の地域のシンクライアントサーバにアクセスした場合に発生するおそれがある問題を，ネットワークに関連する要因とともに 50 字以内で述べよ。

設問 6　本文中の下線⑧について，(1)，(2)に答えよ。

(1)　ID とパスワードの再入力が必要である地域を，本文中の用語を用いて答えよ。

(2)　SSO を実現するためには，どの構成要素に対して，どのような設定が必要か。設定が必要な構成要素を二つ選び，答えよ。また，それらの設定内容を，それぞれ 15 字以内で述べよ。