問1　認証・認可基盤構築の実施計画に関する次の記述を読んで，設問1～4に答えよ。

X社は，従業者数10,000名の大手小売業である。X社は，各事業組織の独立性が高く，それぞれが必要な業務システムを開発し，情報システム部は主に基盤の提供，業務システムの開発ガイドラインの提供及び業務システムの運用管理を行っている。CIOは，ITガバナンスが不十分であると認識しており，効率的なIT運用を図ると同時に，セキュリティ管理の強化や技術標準の確立などを急ぐ必要があると考えている。

X社は戦略的に経営統合を行い，成長を図ってきた。現在，Y社と1年後の経営統合を目指して交渉を進めている。

X社の経営トップは，経営統合のためには，統合両社の従業者による情報共有や連携作業を安全にかつ効率よく行う必要があると考えている。そこで，CIOは，情報システム部に対して，IT施策の実施を加速し，Y社との経営統合に間に合わせるよう指示を出した。情報システム部では，プロジェクトチーム（以下，Pチームという）を編成して検討を始め，まず，認証・認可基盤の構築が必要であると判断し，CIOに報告した。CIOの承認を受け，Pチームは認証・認可基盤構築の実施計画を策定する作業に入った。

〔X社情報システム群の概要と認証・認可基盤構築の基本方針〕

X社には，図1に示す大小合わせて100の業務システム（以下，X社情報システム群という）が存在する。多くのシステムは，Web技術に基づいたもの（以下，Web方式という）であるが，基幹業務システムの一部には，Web方式でない独自技術に基づくクライアントサーバ方式（以下，C/S方式という）も存在する。C/S方式の業務システムについては，今年度後半に，Web方式に再構築することを計画している。

現行の業務システムには，購買システムのように，アプリケーションプログラムに認証機能が組み込まれているもの（以下，アプリ認証方式という）と，研究開発システムのように，アプリケーションプログラムが稼働しているWebサーバの前段にリバースプロキシ型の認証サーバを設置しているもの（以下，プロキシ認証方式という）がある。

Pチームでは，これまでのX社情報システム群の問題を洗い出し，認証・認可基盤構築についての基本方針を決定するために集中検討会を行うことにした。

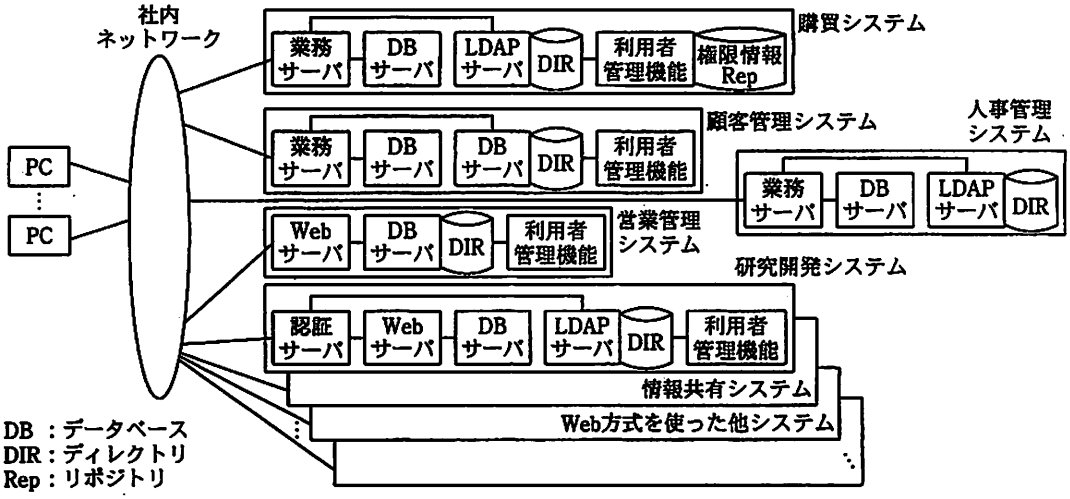


図 1　X 社情報システム群の概要

集中検討会では，利用者認証，アクセス権付与管理，利用者認証・認可に用いるディレクトリ（以下，ディレクトリという）の統合，利用者認証・認可に用いる情報（以下，利用者情報という）の維持管理の 4 点について現状と問題を整理し，改善策の検討を行った後，Y 社との経営統合に備え，Y 社の従業者による X 社情報システム群の利用について検討を行うことにした。

〔利用者認証に関する現状と問題〕

利用者 ID 体系については，従業者番号に基づいた利用者 ID を使用している業務システムが多いが，従業者の氏名に基づいた利用者 ID を使用している業務システムもある。そのため，利用者は，各業務システムに利用者 ID，パスワードなどを入力する際に混乱したり，覚えきれなかったりするという問題が起きている。

〔アクセス権付与管理に関する現状と問題〕

X 社では，組織変更に伴う役職に対する役割や職掌の変更が頻繁に発生する。例えば，請求書にかかわる業務は，現在は営業部の担当であるが，過去には営業部と独立した，ほかの組織が担当したこともあった。また，組織横断的なプロジェクトチームが組織されて業務を遂行することも多く，従業者が複数の組織に属したり，複数の役割を同時にもったりすることも，しばしば発生している。そのため，1 人の従業者による業務システムへのアクセスでも，所属組織や役割によって，使用できる機能を限

定することが必要になってきている。

さらに，以前から，業務システムによっては不必要なアクセス権が利用者に与えられていて，セキュリティ上好ましくないという意見があった。

〔ディレクトリの統合に関する現状と問題〕

現在の X 社情報システム群の業務システム名，システム方式，認証方式，ディレクトリの実現方法，登録されている利用者 ID 数及び利用者情報を表に示す。

ディレクトリについては，業務システムごとに構築され維持運用されているので，統合化などによって，運用効率及びコストの改善を図るよう CIO から指示されている。そこで，P チームでは，標準技術である LDAP 規格に準拠しているディレクトリは統合できるのではないかと考え，調査を行った。しかし，①LDAP を使用する業務システムを調査した結果，いずれも LDAP 規格に準拠した製品を使用しているにもかかわらず，ディレクトリを容易に統合できないということが分かった。

表　X社情報システム群の業務システム一覧とディレクトリの実現方法など

業務システム名	システム方式	認証方式	ディレクトリの実現方法	利用者 ID 数	利用者情報
購買	C/S 方式	アプリ認証方式	LDAP	4,000	LDAP 標準スキーマに加え，拡張属性として“担当業務”を定義して使用
顧客管理	C/S 方式	アプリ認証方式	独自	5,000	RDB の列として，利用者 ID，パスワード，権限区分を定義して使用
人事管理	C/S 方式	アプリ認証方式	LDAP	3,000	LDAP 標準スキーマである“inetOrgPerson”を使用
営業管理	Web 方式	アプリ認証方式	独自	6,000	RDB の列として，利用者 ID，パスワード，権限区分を定義して使用
研究開発	Web 方式	プロキシ認証方式	LDAP	1,000	LDAP 標準スキーマに加え，拡張属性として“研究区分”を定義して使用
情報共有	Web 方式	プロキシ認証方式	LDAP	10,000	LDAP 標準スキーマを使用。X 社従業者全員にアクセス権付与
⋮	⋮	⋮	⋮	⋮	⋮

〔利用者情報の維持管理に関する現状と問題〕

次に P チームは，利用者情報である利用者の認証情報（利用者 ID，パスワードなど）と認可情報（アクセス権付与などの設定情報）の維持管理について，現状と問題を調査した。

現状では，利用者認証・認可機能は，業務システムごとに個別に実装されており，利用者情報も，業務システムごとに維持運用されている。

各業務システムの利用者情報の維持管理は，システムごとに決められたシステム管理者によって行われている。業務システムを新たに利用開始する従業者は，その業務システムの管理者に対して，利用者情報の登録申請を行っている。

利用者情報の業務システムへの登録及び削除は，小規模な業務システムでは，システム管理者が管理台帳に基づいて手作業で行っているが，購買システムなどの基幹業務システムでは，個別に開発した利用者管理機能で行っている。利用者 ID の新規作成やアクセス権の追加が必要になった場合には速やかに処理が行われるものの，②利用者 ID やアクセス権の一部が不要になった場合に，その削除処理が忘れられることがしばしばある。

以上のとおり，検討項目 4 点について現状と問題を整理した。これらの問題を解決するために，P チームでは，まず，実際のアクセス権付与の状況を具体的に調査することにした。

〔主要業務システムにおけるアクセス権付与状況の調査〕

調査には，システムモデリングの手法を用いることにし，職務の遂行者を抽象的に類型化したアクタ（例えば，営業部員，営業部長）ごとのアクセス権付与状況を洗い出した。具体的には，システム再構築を予定している購買システム及び顧客管理システム，並びに企業活動の中心となる営業管理システムに絞り，アクタごとのアクセス権付与の状況について調査を行った。購買システムは購買部で，顧客管理システム及び営業管理システムは営業部で使用されている。

P チームは調査結果を図 2 のとおり整理した。業務機能は，業務対象と業務操作から成っている。例えば，顧客管理システムでは，顧客情報という業務対象に対して入力更新という業務操作を行う業務機能があり，その業務機能に対するアクセス権が，アクタである営業部員に付与されている。営業管理システムにおいては営業部長に対して，購買システムにおいては購買部長に対して，すべての業務機能に対するアクセス権が付与されている。P チームでは，営業部長及び購買部長に付与されているアクセス権が本当に必要なのかどうか，確認すべきであると考えた。

購買システム				
業務機能		アクタ		
業務対象	業務操作	購買事務員（派遣従業者）	購買部員	購買部長
購買依頼書	同意	○	○	○
発注起案書	照会	○	○	○
	処理	○	○	○
支払請求書	管理	○	○	○
	申請	○	○	○
	承認	－	－	○

営業管理システム				
業務機能		アクタ		
業務対象	業務操作	営業事務員（派遣従業者）	営業部員	営業部長
見積書	作成	○	○	○
	承認	－	－	○
契約書	作成	○	○	○
	発行申請	－	○	○
	発行承認	－	－	○
請求書	作成	○	○	○
	発行承認	－	－	○
売上報告書	申請	－	○	○
	承認	－	－	○
購買依頼書	申請	○	○	○
	承認	－	－	○

顧客管理システム				
業務機能		アクタ		
業務対象	業務操作	営業事務員	営業部員	営業部長
顧客情報	入力更新	－	○	－
	閲覧	○	○	○
	削除	－	○	－

〔凡例〕
○：アクセス権あり　－：アクセス権なし

図２　業務システムにおけるアクタごとのアクセス権付与の状況（抜粋）

そこで，従業者による業務の実態についてヒアリング調査を行い，ユースケース図を使って図３のとおり整理した。

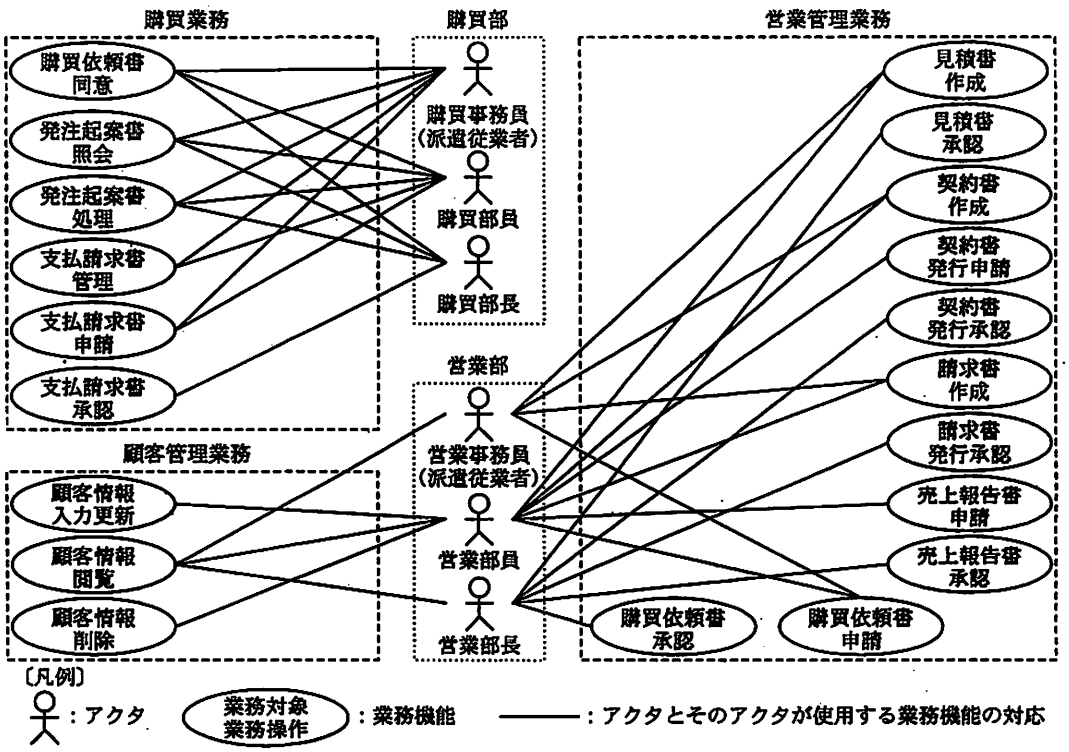


図３　業務の実態についてのヒアリング調査結果（抜粋）

図 3 のユースケースは，業務システムの業務機能と，その業務機能を使用するアクタを示している。図 3 を職務規程と照らし合わせたところ，問題になる利用実態はなかった。

次に，この図 3 を用いて，内部統制上の問題がないか，また，図 2 に過剰なアクセス権付与がないかを分析した。

購買業務では，営業部が発行した購買依頼書に対し，購買部員が発注基準に従って，購買同意又は購買不同意の決定を行い，これを購買依頼書同意機能を使って処理する（業務量が多い場合には部長も当業務を行う場合がある）。購買同意の場合には，発注起案書の申請を購買部員又は購買事務員（派遣従業者）が発注起案書処理機能を使って行い，同じ発注起案書処理機能を使って購買部長が承認の処理を行う。③この購買業務には，アクセス権付与の問題はなかったが，内部統制上の問題が見つかった。そこで，購買部で職務規程を見直してもらい，その結果に基づいて，情報システム部で，どのように業務システムで対応すべきか検討することになった。

営業部の業務には，顧客管理業務と営業管理業務がある。顧客管理業務は，顧客情報を保守する業務である。X 社では，顧客ごとに 1 人又は複数の担当の営業部員が付いている。顧客情報の入力更新及び削除に関する業務は，営業部長は実施せず，個々の顧客を担当する営業部員だけが実施している。この業務には内部統制上の問題もアクセス権付与の問題もなかった。

営業管理業務については，事前に営業部長の申請によって，部長の代行を務める営業部員にアクセス権が付与され，営業部長が不在の際，業務機能を使用する場合がある。営業部の業務には，内部統制上の重大な問題はなかったが，アクセス権付与に関して問題が見つかった。

〔利用者認証に関する問題の解決〕

P チームは，今年度後半，すべての業務システムを Web 方式に再構築し，シングルサインオン（以下，SSO という）を導入することで，X 社情報システム群の現状の利用者認証に関する問題の解決を図ることにした。

〔アクセス権付与に関する改善策の検討〕

P チームでは，調査を通して，組織変更や職掌変更などに伴うアクセス権付与管理を効率的に行うための仕組みが必要であるという結論に至り，各種アクセス制御の方式を比較検討した。その結果，業務に必要な最小限のアクセス権だけを付与することが実現しやすくなり，組織変更や職掌変更などに伴うアクセス権付与管理を効率的に行えるという理由で，ロールベースのアクセス制御を選ぶことにした。ロールベースのアクセス制御では，アクタに対するアクセス権をロールという単位で付与する。ここでロールとは，組織内における一定の権限や責任を伴う業務上の役割を意味する。

P チームでは，一つ以上の業務対象と一つ以上の業務操作との組合せに対するアクセス権をロールとして定義することにした。手始めに，営業管理システムにおける営業部長用のロールについて検討を行った。営業管理システムでは営業部長に一つ以上のロールが定義できると考え，図 4 に示す定義案を作成し，議論した結果，案 4 を採用することにした。

案 1

業務機能		営業部長用ロール群
業務対象	業務操作	営業部長ロール 1
見積書	作成，承認	○
契約書	作成，発行申請，発行承認	○
請求書	作成，発行承認	○
売上報告書	申請，承認	○
購買依頼書	申請，承認	○

案 2

業務機能		営業部長用ロール群		
業務対象	業務操作	営業部長ロール 2-1	営業部長ロール 2-2	営業部長ロール 2-3
見積書	作成，承認	○	－	－
契約書	作成，発行申請，発行承認	○	－	－
請求書	作成，発行承認	－	○	－
売上報告書	申請，承認	－	－	○
購買依頼書	申請，承認	－	－	○

案 3

業務機能		営業部長用ロール群
業務対象	業務操作	営業部長ロール 3
見積書	承認	○
契約書	発行承認	○
請求書	発行承認	○
売上報告書	承認	○
購買依頼書	承認	○

案 4

業務機能		営業部長用ロール群		
業務対象	業務操作	営業部長ロール 4-1	営業部長ロール 4-2	営業部長ロール 4-3
見積書	承認	○	－	－
契約書	発行承認	○	－	－
請求書	発行承認	－	○	－
売上報告書	承認	－	－	○
購買依頼書	承認	－	－	○

〔凡例〕
○：アクセス権あり　－：アクセス権なし

図 4　営業管理システムにおける営業部長用ロールの定義案（抜粋）

ほかの業務システムにおいても，案 4 と同様の考え方に基づいてロールの定義を行う方針にした。P チームでは，ロールベースのアクセス制御を実現するために，④人事管理システムへの管理項目の追加と人事管理システムの運用見直しを行うことにした。

〔Y 社従業者へのアクセス認可方式の検討〕

次に，P チームは，Y 社の従業者に，X 社情報システム群へのアクセスを認可する方式について検討を行った。Y 社との経営統合では，顧客情報などを共有することが想定されている。顧客情報などを共有するための要件は二つある。まず第一に，X 社情報システム群は，Y 社情報システムの利用者認証結果に基づいて，Y 社従業者に X 社情報システム群へのアクセスを認可する。第二に，同様に，Y 社の情報システム群は，X 社従業者に，Y 社の顧客情報を管理する情報システム群へのアクセスを認可する。このようなことを実現する技術の一つに ID 連携技術があるという意見が出た。ID 連携技術とは，お互いに信頼する組織間で，それぞれが管理する利用者の利用者 ID を結び付けることによって，複数の組織間のシステム利用において，利用者認証が一度だけで済む SSO を実現する技術である。

P チームは，検討した結果，ID 連携技術を採用する方針に決めた。

〔ID 連携技術の検討〕

P チームの中で ID 連携技術検討の担当となった E 君は，ID 連携技術の選定について，セキュリティコンサルタントの F 氏に助言を求めた。次は F 氏の E 君への説明である。

F 氏：私は，SAML（Security Assertion Markup Language）2.0 という標準技術を使った ID 連携のシステム構築の経験があります。SAML 2.0 では，異なる製品間の相互運用性について，技術標準を策定する団体が主導して試験を行い，検証結果を公表しています。

E 君：相互運用性が高い技術であれば，X 社の技術標準として採用しやすいですね。

F 氏：そうですね。仕組みについてご説明します。図 5 が，SAML 2.0 を使って SSO を実現する場合のメッセージフローです。この図にある SP（サービスプロバイ

ダ）は，認証された利用者に対して業務アプリケーションなどのサービスを提供する側の機能で，IDP（ID プロバイダ）は，利用者認証の結果を SP に提供する機能です。利用者が SP 上の Web アプリケーションを利用する場合に，SP が利用者に対して Web アプリケーションのサービスを提供してよいかを判定する必要がありますが，この判定のために SP は［ a ］をブラウザ経由で IDP から受け取ります。

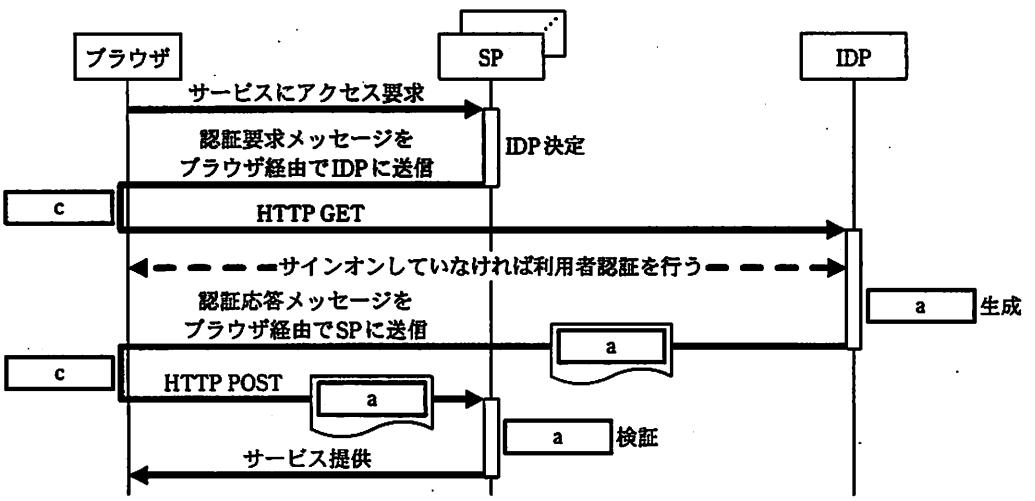


図 5　SAML 2.0 による SSO のメッセージフロー

E 君：なるほど，分かりました。

F 氏：Y 社にも SAML 2.0 の SP を導入したとします。この場合，X 社の利用者が，X 社情報システム群の認証サーバ，つまり，IDP で一度認証を受ければ，［ b ］するまでは，X 社と Y 社の Web アプリケーションは，利用者が個別にサインオンしなくても利用可能となります。

検証済製品には Y 社が導入しているものも含まれており，Y 社と協議した結果，2 社間での ID 連携には問題がないことが判明した。そこで，P チームは，SAML 2.0 を採用することに決めた。

〔X 社情報セキュリティポリシの改訂〕

P チームでは，セキュリティ強化及び IT による内部統制の強化を図り，認証・認可基盤との整合性を確保するために，X 社の情報セキュリティポリシを改訂すべきであると考えた。図 6 に改訂した情報セキュリティポリシ（以下，改訂ポリシという）（案）の改訂部分を示す。改訂ポリシ（案）は P チームでの確認と情報システム部内での審査を経た後，経営会議で正式に承認され，2 か月後に発効することになった。P チームは，各業務システムに対して，発効後 1 年以内に改訂ポリシに準拠するように求めることとした。

（省略）
<K-2. 情報システム利用者の識別，認証及び認可>
(K-2-1) 情報システムの利用者には，利用者の役割や職務に応じた業務上の必要性に基づいて，必要最小限のアクセス権を与えること。
(K-2-2) 情報システムは，権限の分離原則に基づき利用すること。
(K-2-3) 利用者にアクセス権を付与する業務は，次に示すように適正に行うこと。
（以下，省略）

図 6　X 社の改訂ポリシ（案）の改訂部分

〔認証・認可基盤の全体方式の決定〕

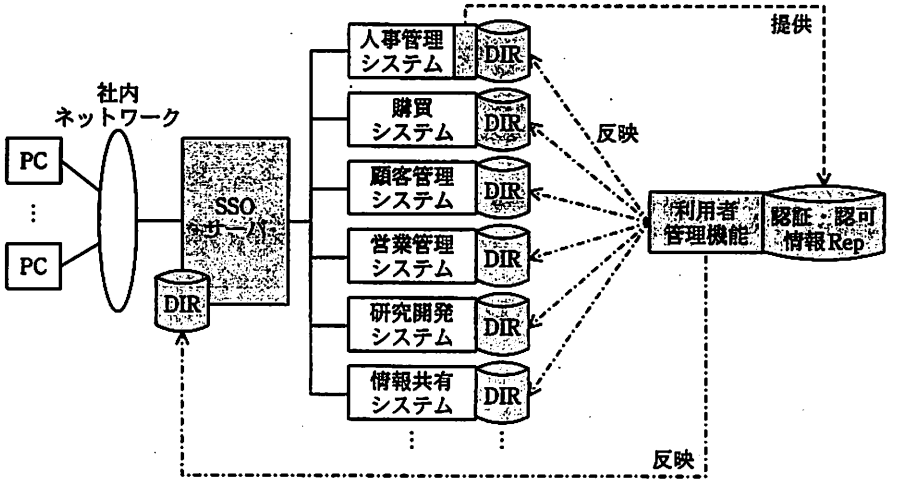
P チームでは，認証・認可基盤の全体方式を決定するために議論を重ねた。次は，P チームのリーダである G 主任とメンバの H さんの会話である。

G 主任：現行の業務システムの利用者認証方式を SSO に統一し，各業務システムを SP として構築するためにはどのような変更や作業が必要か説明してくれないか。

H さん：アプリ認証方式の場合には，プログラムの構造をかなり変更する必要があるので，移行作業には時間が掛かりそうですが，技術的な問題はなさそうです。プロキシ認証方式の場合には，Web サーバの接続先を，今まで使用していた認証サーバから，SSO サーバに切り替えます。各 Web サーバが SSO サーバのインタフェースに対応可能であることは調査済ですので，容易に移行が可能だと思います。いずれの方式でも，SSO を実現するためには ID 連携技術に対応したソフトウェアを追加で導入します。

G主任：Y社との経営統合への対応を含め，利用者認証については，移行についても技術的にめどが立っているようで安心したよ。しかし，利用者情報の維持管理に関しては，どのような方式にするのがよいのかね。

Hさん：総合的に考えて，図7に示す方式がよいと思います。人事管理システムから提供される利用者に関する情報と図4で検討したロールの定義を認証・認可情報リポジトリで一元管理します。それを利用者管理機能によって，SSOサーバと各業務システムのディレクトリに反映させます。



注　網掛けは，認証・認可基盤を表す。

図7　X社情報システム群の認証・認可基盤の全体方式

G主任：そうすると，各業務システムの対応は，どうなるのかね。

Hさん：SSO対応以外にも個々の業務システムの⑤システム改修と運用見直しが必要です。

G主任：分かった。検討作業を続けてくれたまえ。

以上のようにして，Pチームによる集中検討会は終了し，認証・認可基盤構築の実施計画が社内に発表され，認証・認可基盤の構築が開始された。

設問1　ID連携技術について，本文中及び図5中の［　a　］，［　b　］に入れる適切な字句を，それぞれ10字以内で答えよ。また，図5中の［　c　］には，ブラウザにおける動作を示す適切な字句を8字以内で答えよ。

設問2　X社情報システム群の問題について，(1)，(2)に答えよ。

(1) 本文中の下線①について，LDAP規格に準拠しているディレクトリを容易に統合できない理由を，40字以内で述べよ。

(2) 本文中の下線②の現状がもたらすセキュリティ上の問題を，40字以内で述べよ。

設問3　X社情報システム群の主要業務システムにおけるアクセス権付与状況の調査と改善策の検討について，(1)～(4)に答えよ。

(1) 図3を参照して，顧客管理業務について営業部長に付与されるロールに許可すべき業務対象及び業務操作を答えよ。

(2) 本文中の下線③の問題を解決するためには，発注起案書処理機能を二つに分離すべきである。その理由を，内部統制上の観点から60字以内で述べよ。

また，どのように分離すべきか。分離後の発注起案書処理のユースケースについて，“業務操作”と“アクタとそのアクタが使用する業務機能の対応”を図3に倣って示せ。

(3) 営業管理システムの営業部長用ロール定義案として案4が選ばれた理由を二つ挙げ，それぞれ45字以内で述べよ。

(4) 本文中の下線④について，追加される管理項目を10字以内で答えよ。また，運用見直しの内容について，50字以内で具体的に述べよ。

設問4　本文中の下線⑤について，営業管理システムを例にとり，システム改修の内容を二つ挙げ，それぞれ40字以内で述べよ。