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，セキゴ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μ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。

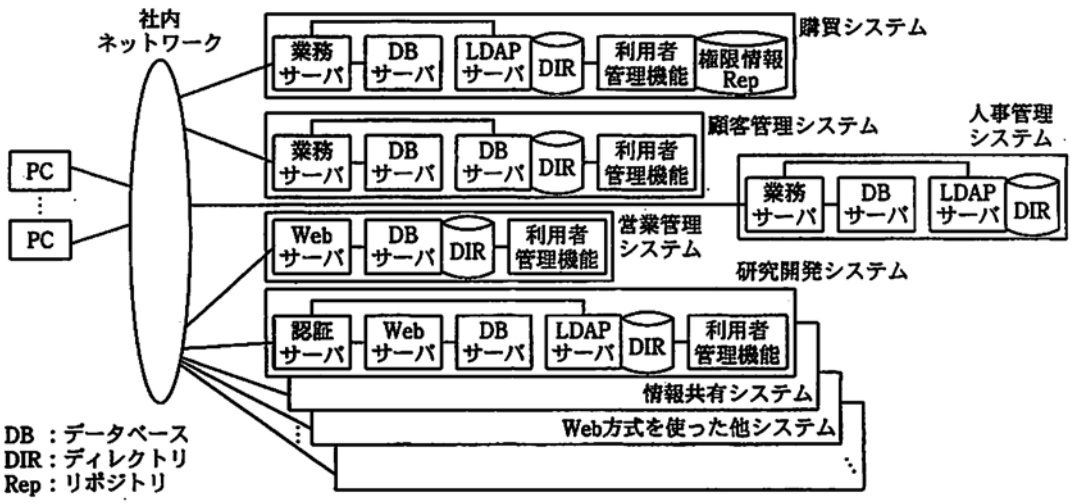


図 1　X 社情報システム群の概要

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，業務システムによづ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	－	－	○

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	－	○	－

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	－	－	○

〔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。

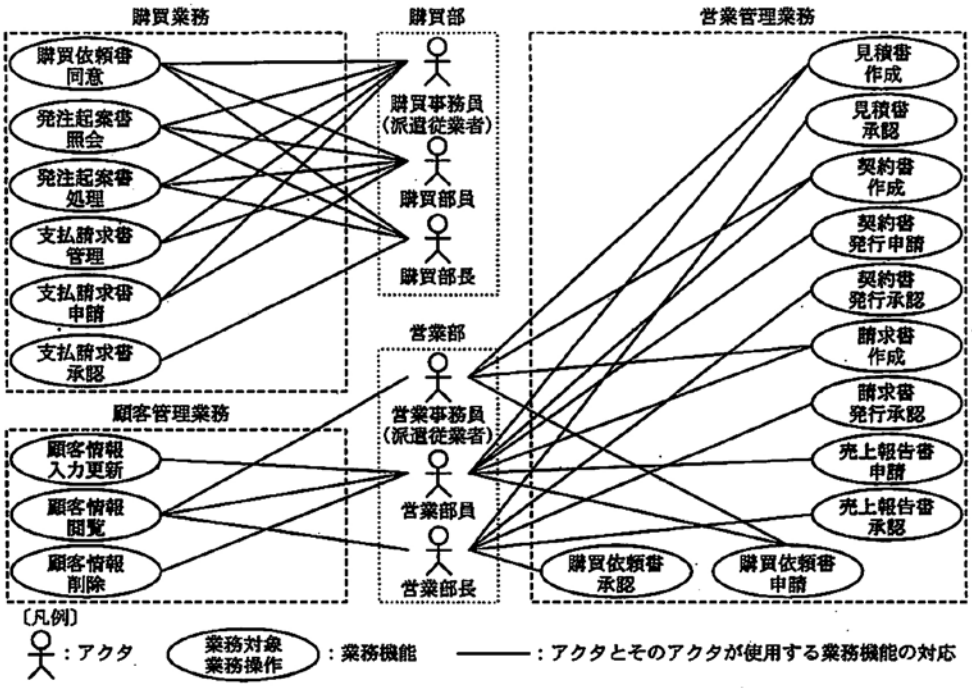


図 3　業務の実態についてのヒアリング調査結果（抜粋）

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（サーピスプロバイダ）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。

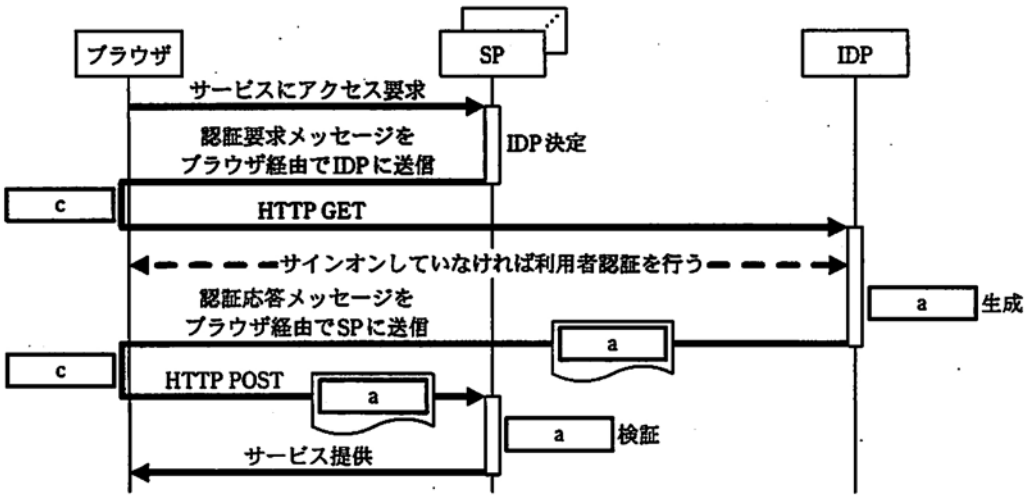


図 5　SAML 2.0 による SSO のメッセージフロー

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)

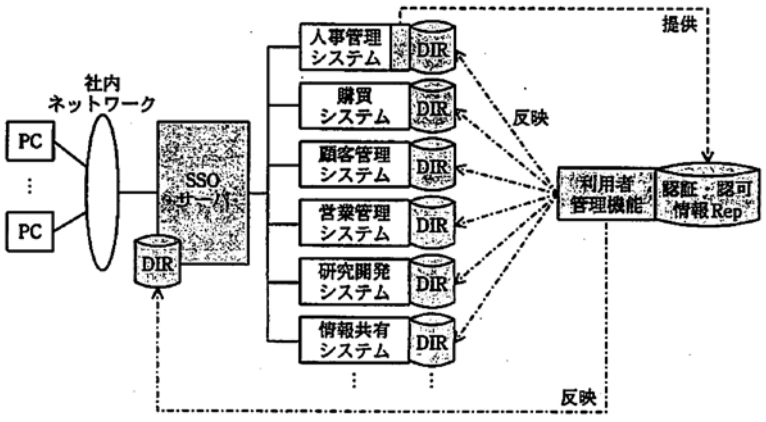
P チームでは，認証・認可基盤の全体方式を決定するために議論を重ねた。次は，P チームのリーダである G 主任とメンバの H さんの会話である。

G 主任：現行め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 中め [c] には，プ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)本文中め下線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。

問 2　社内 LAN の見直しに関する次の記述を読んで，設問 1〜5 に答えよ。

A 社は，従業員数 1,000 名の電子部品メーカである。都心に本社，郊外に工場があり，全国の主要都市に拠点オフィス（以下，本社，工場，拠点オフィスを事業所という）をもつ。本社には，営業部，総務部及びシステム部があり，拠点オフィスには，営業部に所属する従業者（従業員，派遣従業員及びアルバイト）が常駐している。工場には，総務部，システム部，設計部及び製造部がある。

A 社の主力製品は，独自の先端技術を用いた電子部品であり，CAD システムを用いた設計を行っている。近年では顧客の要望にこたえた特注品も生産するようになり，高い技術力と短納期で売上を伸ばしている。

A 社では，受注，生産及び出荷データを管理するネットワーク（以下，S ネットワ

ークという）と設計データを管理するネットワーク（以下，T ネットワークという）を利用している。S ネットワークには本社業務サーバと工場業務サーバなどが接続され，T ネットワークには開発サーバと製造サーパなどが接続されており，二つのネットワークはつながっていない。

〔セキュリティ区画の構成〕

A 社のセキュリティ区画の定義を表 1 に示す。

表 1　A 社のセキュリティ区画の定義

名称	定義	該当するエリア
極秘区画	極秘情報及び機密情報を取り扱う領域	サーバエリア
		設計エリア
機密区画	機密情報を取り扱う領域（例外的に極秘情報を保有又は通過させる場合には適切な対策を施す）	執務エリア
一般区画	原則として極秘情報及び機密情報を取り扱わない領域（例外的に極秘情報又は機密情報を保有又は通過させる場合には適切な対策を施す）	作業エリア

本社は，サーバエリア及び執務エリアから構成されており，拠点オフィスは，執務エリアだけで構成されている。工場は，サーバエリア，設計エリア，執務エリア及び作業エリアから構成されている。極秘情報とは，機密性が極めて高く，設計部など一部の従業員にしか開示しない情報で，開発中の製品データや高度な技術的ノウハウが含まれる。機密情報とは，極秘情報に次いで機密性が高く，発注者である顧客などとの間で機密保持契約が結ばれている場合だけ当該顧客に開示できる情報で，受注情報や生産管理情報が含まれる。設計部員は，極秘情報及び機密情報を扱う場合は設計エリアで作業を行っている。

機密区画への立入りは，磁気カードによる認証が必要である。極秘区画への立入り及び退出の際には，磁気カードによる認証に加えて指紋認証も必要である。一般区画への立入りについては，特別な認証制限を行っていないが，工場においては，敷地外から敷地内に入る際に，外来受付で従業員証又は入構証の提示による入構管理を行っている。従業員証と入構証のどちらも保持していない場合には，その都度，臨時の入構証が発行される。各エリアの業務従事者を表 2 に示す。

表 2　各エリアの業務従事者

エリアの名称	業務従事者
サーバエリア	システム部に所属する従業員
設計エリア	設計部に所属する従業員
執務エリア	総務部，営業部及び製造部に所属する従業者
作業エリア	製造部に所属する従業者，運送業者など

A 社の情報セキュリティポリシでは，次のことを規定している。

・極秘情報を保存するサーバが接続された LAN を，機密区画又は一般区画の LAN と接続する場合には，ファイアウォール（以下，FW という）によるアクセス制御を行う。
・機密区画の PC から極秘情報を保存するサーバへのアクセスは，原則禁止するが，許可する場合には，適切なアクセス制御を行う。

〔S ネットワークと内線電話構成の概要〕

S ネットワークは，本社業務サーバが接続された本社 LAN，工場業務サーバが接続された工場 LAN，拠点 LAN 及びこれらの LAN を接続するデータ通信用の専用線で構成されている。S ネットワークと内線電話の構成を図 1 に示す。S ネットワークで取り扱う情報には，機密情報が含まれる。本社 LAN 及び拠点 LAN には，各事業所において使用する業務用の PC（以下，GPC という）が接続されている。工場 LAN には，工場内で使用する GPC のほかに，無線接続が可能な GPC（以下，NPC という）と無線アクセスポイント（以下，AP という）で構成される無線 LAN が含まれる。

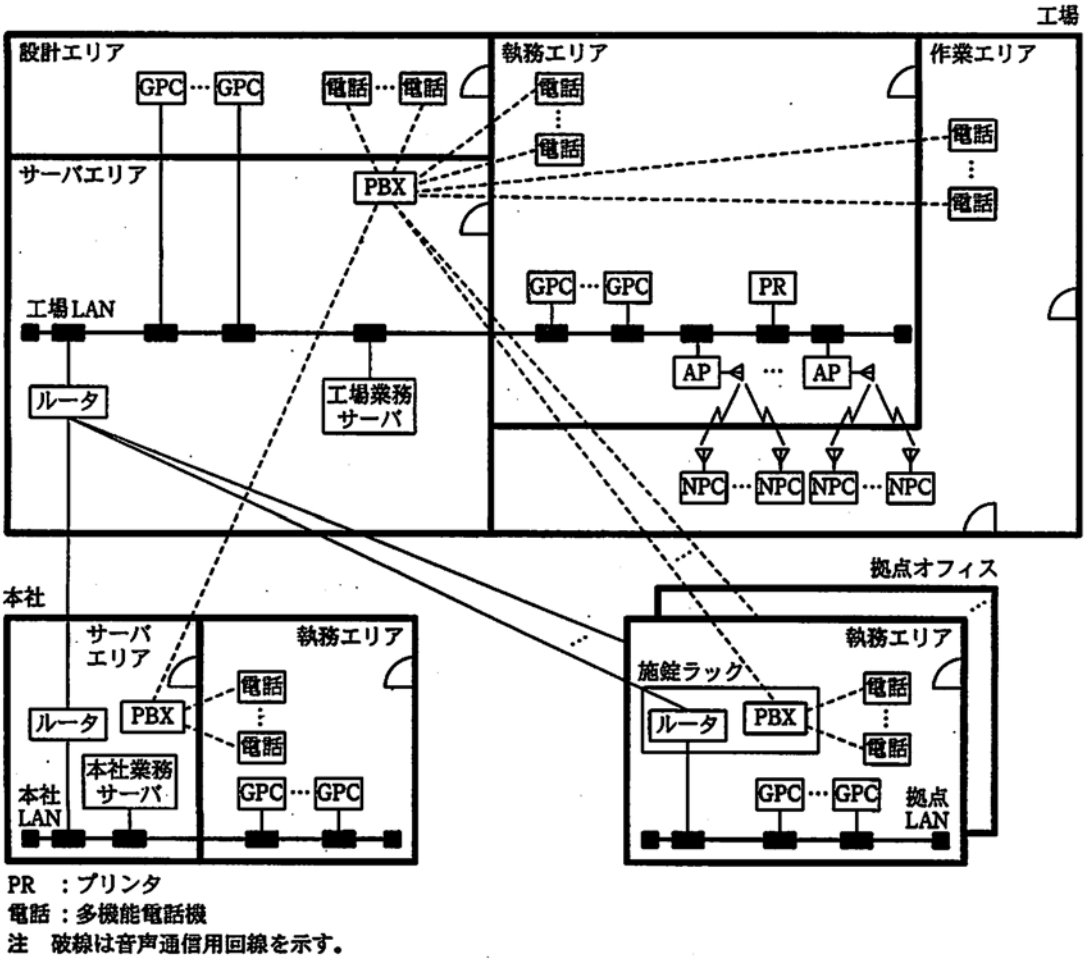


図 1 Sネットワークと内線電話の構成

本社業務サーバでは受注管理アプリケーションが稼働しており，本社及び拠点オフィスの営業担当者は，執務エリアに設置された GPC を用いて，受注管理アプリケーションに受注データを入力する。入力された受注データは，受注管理アプリケーション

の夜間バッチによって集計され，工場業務サーバに転送される。工場業務サーバでは生産管理アプリケーションが稼働しており，集計された受注データは生産データ及び出荷データの二つにまとめられる。生産データは製品型番別の生産数を集計したものであり，出荷データは出荷先の顧客別に製品型番，納品数及び納品日をまとめたものである。工場では，製造部の担当者が，工場の執務エリアに設置された GPC を用いて，生産指示書として生産データの印刷を行い，それに基づいて製品を製造する。完成した製品は，作業エリア内の製品保管庫で保管され，顧客向けに出荷される。工場の製造部の担当者は，NPC から無線 L.AN 経由で工場業務サーバにアクセスし，出荷データに従って製品を出荷する。NPC は共用の PC であり，全員が同じアカウントでログインして使っている。無線 LAN には，WPA2 方式を採用している。生産指示書及び NPC は，作業を行う都度，作業エリアに持ち出して使用し，使用後は執務エリアにおいて保管している。

A 社の内線電話は，各事業所に設置された PBX と電話によって構成されており，各事業所の PBX 間は音声通信用の専用線によって接続されている。

本社業務サーバ，工場業務サーバ，本社と工場のルータ及び PBX は，サーバエリアに設置されている。一方，各拠点オフィスのルータ及び PBX は，施錠ラックに格納され，各拠点オフィスの執務エリアに設置されている。

〔T ネットワークの概要〕

A 社では，CAD システムと連動した製造装置を 5 年前に導入し，設計工程及び製造工程の効率向上を図っている。T ネットワークは，これらの製造装置の導入時に構築されたものであり，開発 LAN 及び製造 LAN で構成されている。開発 LAN には，開発サーバ及び設計エリアの PC（以下，KPC という）が接続されており，開発サーバでは CAD システムの製品開発用アプリケーションが稼働している。製造 LAN には，製造サーバ，執務エリアの PC（以下，SPC という）及び作業エリアの製造装置に組み込まれた PC（以下，MPC という）が接続されている。T ネットワークの構成を図 2 に示す。

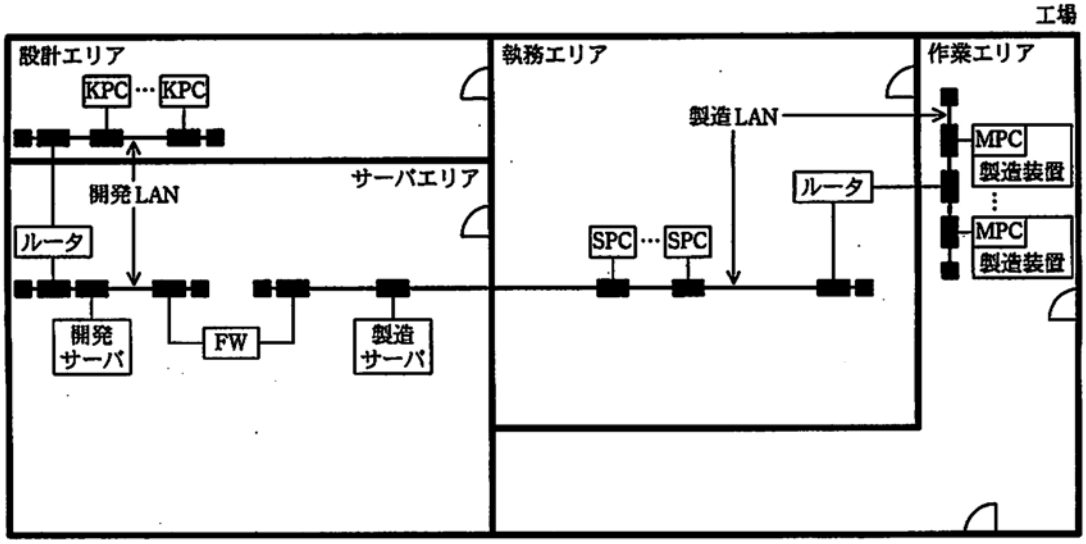


図２　Ｔネットワークの構成

図 2 中の開発サーバに保存される CAD データは極秘情報に該当するので，A 社の情

報セキュリティポリシに従い，開発 LAN と製造 LAN は，FW を介して接続されている。また，製造 LAN の一部は，作業エリア内にも敷設されている。作業エリア内のネットワークケーブルは，電線管によって保護されている。

設計部では，KPC を用いて開発サーバ上の設計中の電子部品に関する CAD データにアクセスし，電子部品の設計を行っている。KPC には，CAD システム専用の端末アプリケーションがインストールされており，開発サーバとは CAD システム固有のプロトコルで接続する。設計部において電子部品の設計が完了し，商品化が決定したら，その製造に用いるデータ（以下，製造データという）は，開発サーバから製造サーバへ移され，製造サーバで管理される。製造部では，SPC から製造データにアクセスし。各種製造装置に製造データを入力して製品を製造する。

T ネットワークの構築当時は，同一規格品の生産が主であり，製造データには極秘情報に該当するものは含まれていなかった。しかし，特注品の生産増大に伴い，製造データには極秘情報に該当する独自のノウハウが含まれるようになってきている。つまり，製造サーバにも極秘情報が保存されてきており，この現状は A 社の情報セキュリティポリシに違反しており，製造 LAN の情報セキュリティ対策がシステム部において大きな課題になっている。

〔A 社の経営課題〕

A 社では，拠点オフィスが増えたことに伴い，内線電話のために設置している専用線の維持費負担が経営課題の一つとなっている。また，顧客からの製品仕様の変更要求に迅速に対応するために，本社又は拠点オフィスの営業担当者と工場の設計担当者との間で迅速に情報連携を行う必要があり，製品仕様変更の打合せでの CAD データの積極的活用が課題となっている。この二つの課題への取組みのため，現在は接続されていない S ネットワークと T ネットワークの統合を含む，社内 LAN の再構築が経営会議で決定された。また，これを契機に，将来のテレビ会議システムの導入も視野に入れて検討するよう指示があった。この社内 LAN の再構築は，システム部が主管となって進めることになった。

〔音声通信とデータ通信の統合〕

まずシステム部では，検討の結果，次の基本方針を定めた。

・音声通信とデータ通信は統合した上で，専用線は IP-VPN に変更する。

・既存の電話は IP 電話端末（以下，IP 電話という）に置き換え，社内 LAN に接続する。

この基本方針を伝えた上で，音声とデータの通信を統合する方式の提案を SI ベンダの B 社に求めた。それに対して B 社からは，SIP を採用した SIP サーバを含むシステム提案があった。

B 社の提案した SIP サーバは，音声通信用のサーバであり，IP 電話のアドレス情報の管理，呼制御及び構内電話交換を行うものであった。接続を確立する過程と接続を切断する過程では，SIP サーバが通信制御に介在し，電話番号から相手の IP アドレスを検索して接続要求を転送するなどの処理を行う。接続が確立されてから切断されるまでの通話を行う過程では，IP 電話同士が直接通信を行う。

工場のネットワーク構成の見直しは，工場のシステム部に所属している C 君が担当することになった。次は，C 君と B 社のセキュリティエンジニアの D 氏の会話である。

C 君：工場では，T ネットワークの FW を通して，S ネットワークと T ネットワーク

を接続することを検討しています。音声とデータの通信を統合する際に注意すべき点を教えてください。

D 氏：IP 電話間の通話に使われるプロトコルである RTP は，UDP ポート番号の使用範囲が広く，かつ，使用するポート番号を動的に割り当てます。そのため，FW のパケットフィルタリングでは，広範囲な UDP ポート番号を許可する必要があります。これに対して，SIP 対応機能をもつ FW（以下，FWx という）がベンダ各社から提供されています。FWx では，通話時に割り当てられたポート番号による IP 電話間のアクセスだけを許可し，それ以外のアクセスを遮断することができます。

C 君：それでは，現在 T ネットワークで使用している FW は，利用を継続することができないのでしょうか。

D 氏：利用を継続することは可能です。しかし，SIP 対応機能をもたない FW は，音声パケットの通信に利用されるポートを動的に開閉することができないので，①FWx に置き換えることの効果は大きいと思います。

C 君：開発 LAN の IP アドレスが，本社 LAN の IP アドレスと重複しているのですが，NAT などのアドレス変換を行う場合についての問題はありませんか。

D 氏：現在の FW でアドレス変換を行う場合には，パケットのルーティングができないので，IP アドレスを一部変更して重複がないようにしておく必要があります。

C 君：分かりました。S ネットワークと T ネットワークの統合を検討する際に考慮することにします。

〔S ネットワークと T ネットワークの統合〕

C 君の検討結果を基に作成した，A 社の新ネットワークの構成を図 3 に示す。

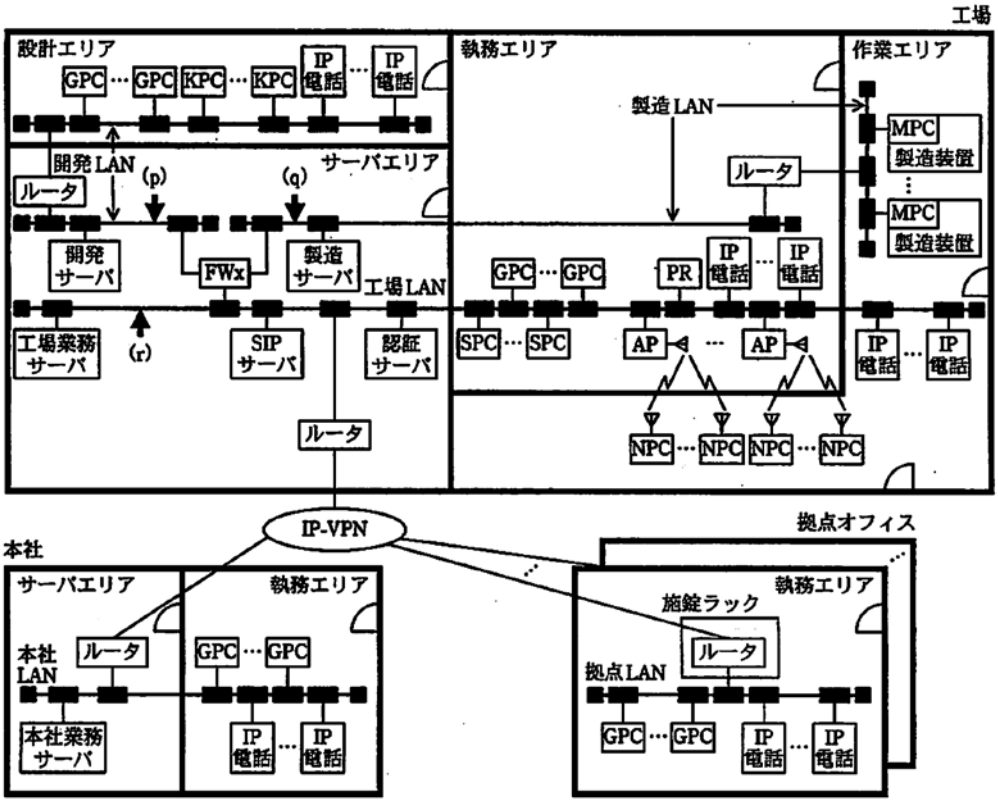


図 3　新ネットワークの構成

C 君は，S ネットワークのプライベートアドレスの振り直しを行うとともに，現在使用中の FW を FWx に置き換え，S ネットワークと T ネットワークを，FWx を介して接続することにした。さらに，営業担当者と設計担当者との間で情報を共有する必要があることから，事業所間において特注品の設計に関するデータを共有するためのサーバ（以下，情報共有サーバという）を，新規に導入することにした。これによって，設計担当者が，営業担当者との設計変更の打合せの際に，極秘情報を削除した共有データを作成して情報共有サーバに保存することで，営業担当者もそのデータを本社及び拠点オフィスから参照できるようになった。

設計エリアの IP 電話と GPC は，開発 LAN に接続することにし，工場の執務エリアの IP 電話及び SPC 並びに作業エリアの IP 電話は，工場 LAN に接続することにした。SPC を工場 LAN に接続することに伴い，②製造 LAN のネ y トワフクケーブルを電線管で保護し，執務エリアの床下に敷設することにした。

また，情報共有サーバの導入に伴い，不正アクセス対策を強化する必要があると考えた C 君は，無線 LAN の認証プロトコルとして IEEE 802.1x 方式を採用することにし，認証サーバを新規に導入することにした。

認証方式については，利用者 ID とパスワードを用いる PEAP 方式と PC に組み込んだクライアント証明書を用いる EAP-TLS 方式を比較し，業務上利用する必要めない従業者が NPC を執務エリアから作業エリアに不正に持ち出して工場 LAN に接続する場合を考慮し，③PEAP 方式を採用することにした。

C 君が作成した FWx のアクセス制御ルールを，表 3 に示す。アクセス制御ルールは，項番順に優先して適用される。

表 3　FWx のアクセス制御ルール

項番	送信元	あて先	サービス	制御
(1)	KPC	製造サーバ	すべて	許可
(2)	SPC	製造サーバ	すべて	許可
(3)	開発 LAN の PC	工場 LAN のサーバ	すべて	許可
(4)	本社 LAN，工場 LAN，拠点 LAN の IP 電話	a	RTP	許可
(5)	a	本社 LAN，工場 LAN，拠点 LAN の IP 電話	RTP	許可
(6)	b	a	SIP	許可
(7)	a	b	SIP	許可
(8)	すべて	すべて	すべて	拒否

注　送信元とあて先については，IP アドレスに代えて PC 名，サーバ名などを記載している。また，KPC と SPC に対しては，固定の IP アドレスが付与されている。

〔セキュリティ対策の検討〕

C 君が作成した案に対して，システム部において検討会議が行われた。検討会議では，NPC を用いた不正接続を検知するためには，日常の管理を強化する必要のあることが指摘された。このため，NPC の管理状況を④定期的に点検し，点検結果と無線 LAN の接続履歴とを照合することにした。

検討会議の結果を反映させた C 君の修正案は承認され，これに基づいて A 社の社内

LAN の再構築が行われ，無事に完了した。

設問 1　表 3 中の [a] ，[b] に入れる適切な字句を・それぞれ 15 字以内で答えよ。

設問 2　本文中の下線①について，DoS 攻撃を想定した場合，FWx に置き換えることによって，どのような効果が期待できるか。35 字以内で述べよ。

設問 3　情報共有サーバについて，(1)，(2)に答えよ。

(1)C 君は，新ネットワークの構成において，情報共有サーバを図 3 中のどこに接続することにしたと考えられるか。最も適切な箇所を(p)〜(r)の中から選び，記号で答えよ。また，選択した箇所以外には接続すべきでない理由を，70 字以内で述べよ。

(2)極秘情報に該当するデータが，情報共有サーバに残存することを防止するために，設計部ではどのような対策を実施すべきか。保存前対策と保存後対策を一つずつ挙げ，それぞれ 40 字以内で述べよ。

設問 4　製造 LAN のセキュリティ対策について，(1)，(21)に|答えよ。

(1)本文中の下線②について，サーバエリアから製造装置までのネットワークケーブルを電線管によって保護するのは，どのようなリスクの低減を意図したものか。ネットワークケーブルが破損すること以外のリスクを，25 字以内で述べよ。

(2)C 君が，工場 LAN と製造 LAN を比較した結果，SPC を工場 LAN に接続すると判断した理由を，90 字以内で述べよ。

設問 5　工場 LAN のセキュリティ対策について，(1)〜(3)に答えよ。

(1)PEAP 方式において，認証情報を盗聴のリスクから保護するために使用されている暗号プロトコルを答えよ。

(2)本文中の下線③について，C 君が，PEAP 方式と EAP-TLS 方式を比較した結果，PEAP 方式を採用すると判断した根拠を，50 字以内で述べよ。

(3)本文中の下線④について，定期点検を実施する前提として必要と考えられる日常の N で PC 運用方法を，35 字以内で述べよ。

解答例

問 1

出題趣旨

情報システムの構築において，情報セキュリティ技術者は，企業の経営戦略に適した技術を選択するとともに，内部統制の観点も併せもって情報セキュリティを確保するための検討を行うことが求められている。

本問では，経営統合に伴うシステム連携を状況として設定し，認証・認可基盤の構築計画策定を題材に，ロールベースのアクセス制御や ID 連携技術の基本的な理解を問うとともに，ID 管理を検討する際に求められる技術及び運用プロセスの両面から総合的に判断し，適切な構築計画を策定する能力を問う。

設問 l　a　・認証アサーション
・認証トークン
b　サインオフ

c　リダイレクト

設問2（1）業務システムごとに拡張属性を定義して使用しており，スキーマが異なるから

（2）・業務システムへのアクセスが本来許されない利用者が，アクセス可能な状態になる。

・退職や異動で権限がなくなったはずの者が業務システムにアクセスできてしまう。

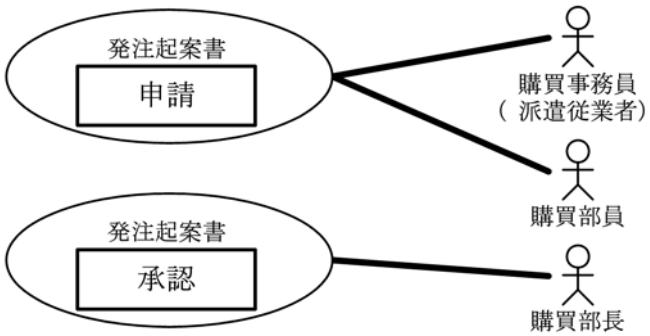
設問3（1）**業務対象**　顧客情報

業務操作　閲覧

（2）**分離すべき**　発注起案書申請と発注起案書承認が同一人物によって行われ，架

理由　空発注などの不正を発見できないおそれかおるから

分離後



（3）①　・職掌変更などで役職に対する役割に変更が発生した場合に，容易に対応できるから

②　・申請と承認のような分離されるべき責務が，同じ権限として定義されていないから

（4）**追加される管理項目**　・ロールに関する情報

・職掌に関する情報

運用見直しの内容　人事部あるいは管理者によって，従業者の所属組織や職掌の変更の都度，遅滞なく，情報を更新する。

設問4　①　・認証方式をアプリ認証方式からプロキシ認証方式に変更する。

②　・認可ロジックをロールベースのアクセス制御に対応した実装にする。

問2

出題趣旨

情報セキュリティの実現に当たっては，取り扱う情報の機密性に応じて適切なセキュリティ対策を講じるとともに，環境の変化に対応して継続的に改善を図る必要かおる。

本問では，内線電話の IP 電話化と情報連携の迅速化という課題への取組みを状況として設定し，ネットワークの統合を含む社内 LAN の見直しを題材に，ファイアウォールによるアクセス制御や無線 LAN の認証技術の基本的な理解を問うとともに，機密性の高い情報を保護するための対策を講じる能力を問う。

設問l　a　開発 LAN の IP 電話　又は　設計エリアの IP 電話

b　SIP サーバ

設問2　DoS 攻撃のパケットを遮断できる可能性が高くなる。

設問 3（1）**接続箇所**　（r）
接続すべきでない理由　極秘情報が保存された開発サーバや製造サーバが接続された開発 LAN 及び製造 LAN に，営業担当者がアクセスすることを許可すべきではないから
（2）**保存前対策**　・共有データを保存する際に責任者が内容を確認して承認する。
・共有データの作成者とは別の担当者が内容を確認して保存する。
・極秘情報と機密情報の区別を明確にして設計部員に周知徹底する。
保存後対策　・極秘データが情報共有サーバに保存されていないことを定期的に検査する。
設問 4（1）・ネットワークケーブルへの PC の不正接続
・ネットワーク上を流れる特注品に関する極秘情報の盗聴
（2）情報セキュリティポリシに従い，機密区画にある SPC から極秘情報を保存することになった製造サーバにアクセスする場合には，FWx によるアクセス制御を行う必要があると判断したから
設問 5（1）SSL 又は　TLS
（2）・PEAP 方式は EAPjrLS 方式に比べて利用者を特定できる利点かおるから
・EAPjrLS 方式はクライアント証明書を組み込んだ PC を認証するので利用者を特定できないから
（3）NPC の持出しと返却の日時及び使用者に関する記録を残すこと

採点講評

問 1

問 1 では，ID 連携を含む，認証・認可基盤の統合について出題した。全体として，正答率は低かった。

設問 1 は，a 及び c の正答率が低かった。 SAML 及び HTTP の標準仕様の中で定義された用語を理解していないと見受けられる解答が多かった。具体的な製品仕様や技術の表層的な理解だけではなく，その標準仕様の全体的な理解も深めてほしい。

設問 2（2）は，正答率が低かった。本文に記述された状況から想定される具体的な問題点を問うたが，削除されずに残った利用者 ID やアクセス権が“悪用される”，“不正アクセスに使われる”といった，あいまいな解答が見受けられた。

設問 3 は，全体では想定どおりの正答率だったが，（4）の運用見直しの内容の正答率は低かった。 ID 管理及びアクセス管理においては，異動・退職といった変更を情報システムに即座に反映させることが重要である。
しかし，図 7 に示された方式を説明しただけの解答，図 7 と矛盾する内容の解答が見受けられた。また，“適切に管理する”といった，あいまいな解答も見受けられた。

設問 4 は，正答率が低かった。本文及び設問でそれぞれ“個々の業務システムのシステム改修”，“営業管理システムを例にとり”と記載しているにもかかわらず，“ID 体系を統一する”，“権限情報を一元化する”，“ディレクトリを統合する”といった，X 社情報システム全体に関する解答が多かった。また，営業管理システムの改修として，認証方式の変更と認可方式の変更の両方が必要であるが，どちらか一方だけに関する解答も多かった。

問 2

問 2 では，ネットワークの統合を含む，社内 LAN の見直しについて出題した。全体として，正答率は想定どおりだった。

設問 2 では，DoS 攻撃を想定した場合における，UDP ポートの動的開閉の効果について記述していない解答が散見された。 IP 電話については，今後，利用がますます促進すると思われるので，関連するセキュリティ対策についても理解を深めてほしい。

設問 3(2)は，正答率が低かった。残存する極秘情報を検知することの重要性を考慮して，解答してほしかった。

設問 4(2)は，正答率が低かった。環境の変化に伴い，製造サーバに極秘情報が保存されるようになったことについて，新たな対応が必要であることを理解していない解答が多く見られた。重要な情報の所在が変化する場合かおり，情報セキュリティ対策の継続的な見直しと改善を図る必要かおることを理解しておいてほしい。

設問 5(2)は，正答率が低かった。 PEAP 方式は EAP 方式を強化したものであり，EAP-TLS 方式と共通の技術を採用しているが，PEAP 方式は利用者 ID とパスワードによって利用者本人を特定できる方式であり，EAP-TLS 方式はクライアント証明書によって PC を特定できる方式である。採用する認証方式によって，認証の対象が異なることについて理解しておいてほしい。