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バ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。

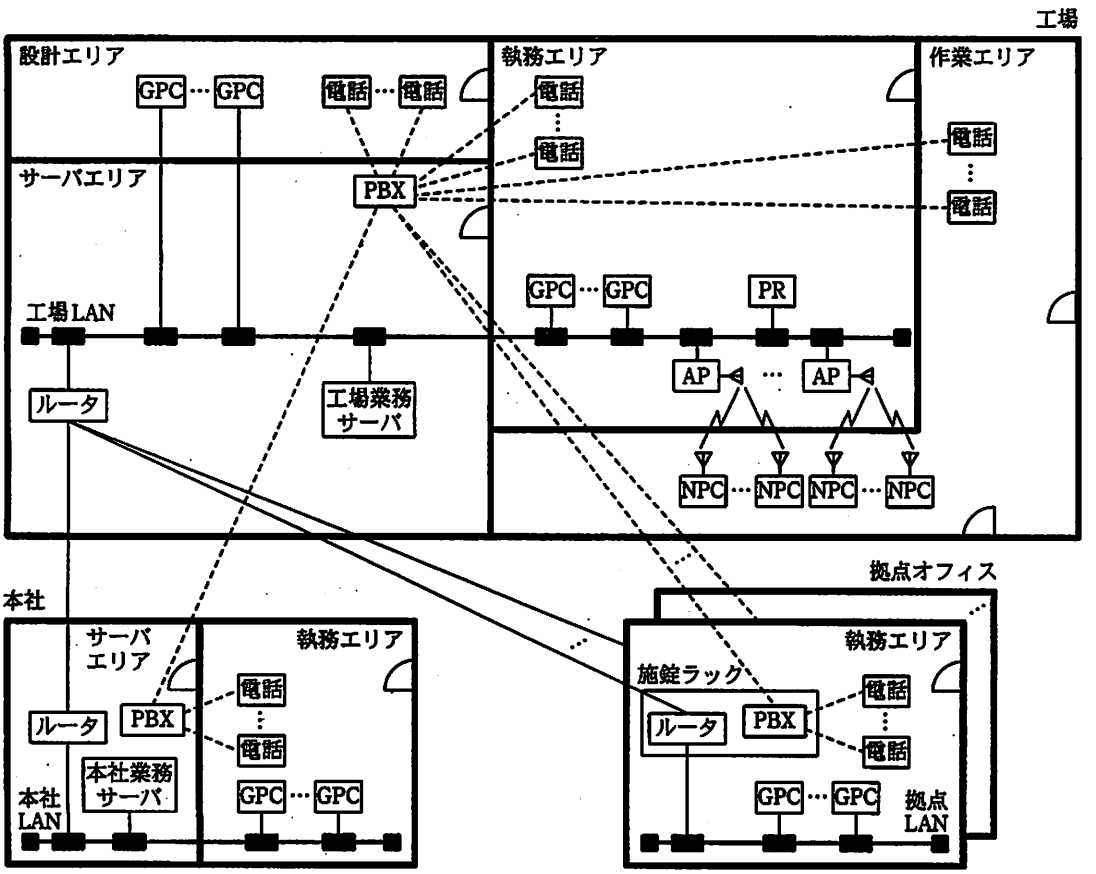
・極秘情報を保存するサーバが接続された LAN を，機密区画又は一般区画の LAN と接続する場合には，ファイアウォール（以下，FW という）によるアクセス制御を行う。

・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。



PR　：プリンタ
電話：多機能電話機
注　破線は音声通信用回線を示す。

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 LAN 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。

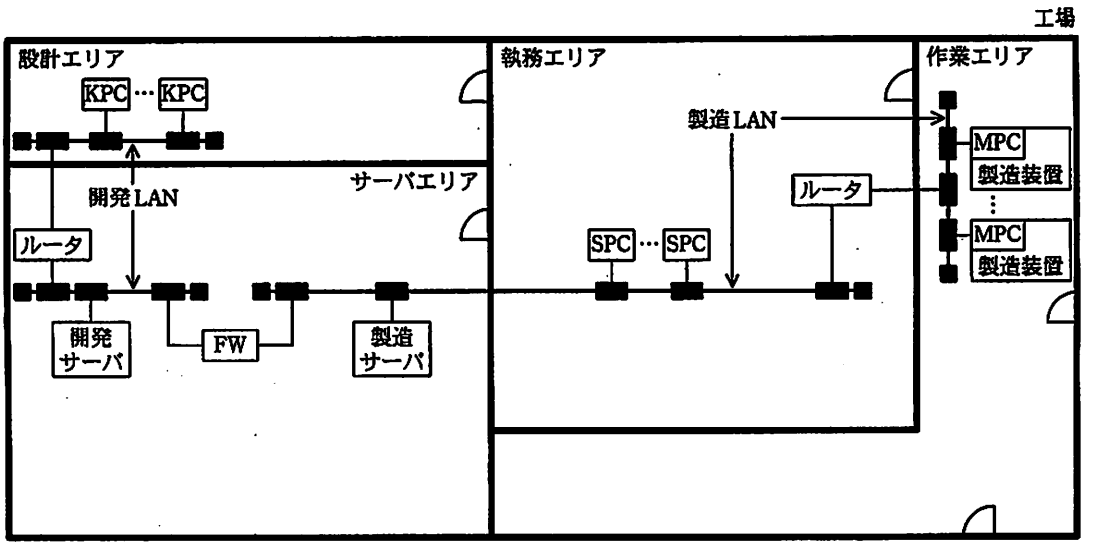


図2　Tネットワークの構成

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。

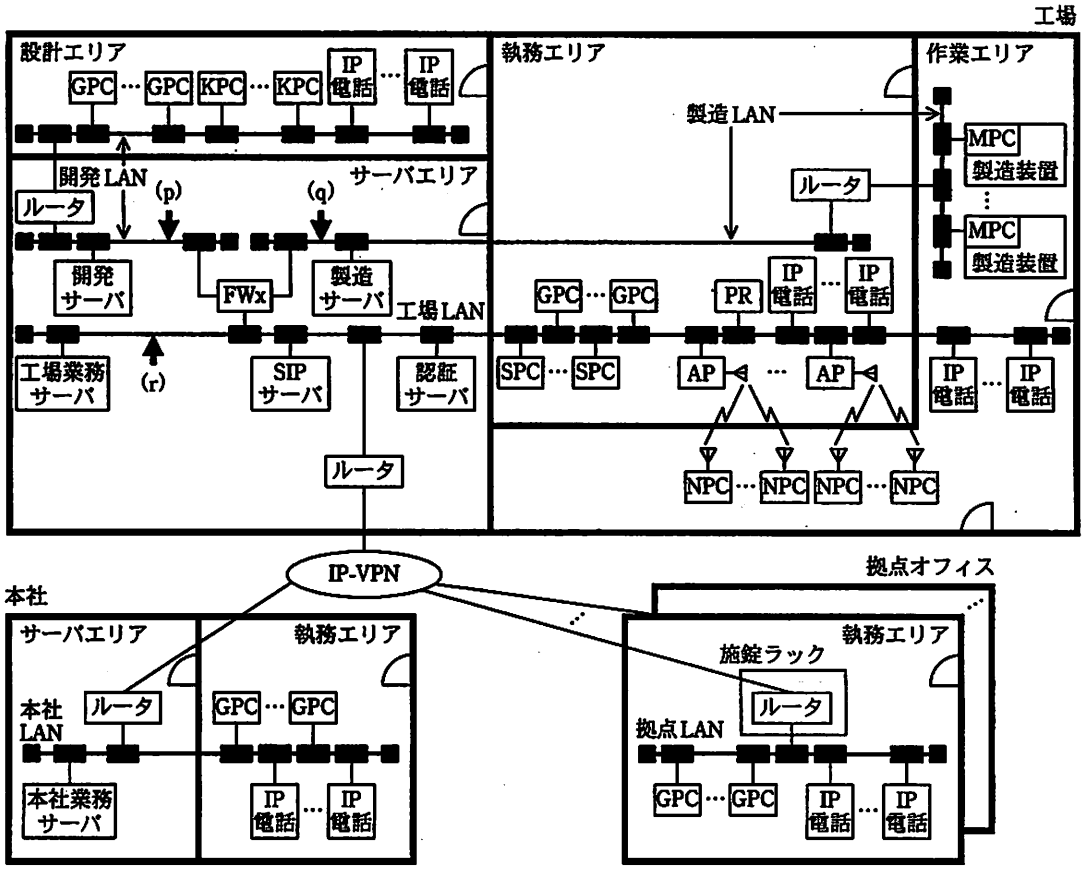


図3　新ネットワークの構成

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 のネットワー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のない従業者が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)，(2)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NPC運用方法を，35字以内で述べよ。