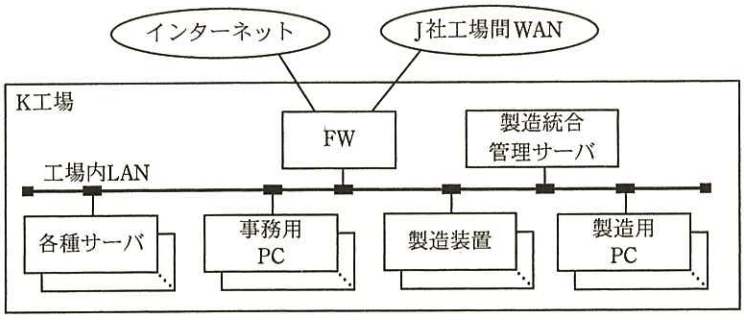
問2　製造業におけるネットワーク構築に関する次の記述を読んで，設問 1～4 に答えよ。

J 社は金属製品製造会社である。J 社の主力工場である K 工場は，20 年前に開設されて以来，製造ラインで様々な製品を生産しており，現在 400 名の従業員が働いている。K 工場では合理化の一環として，製造装置の LAN 接続を進めていた。

〔K 工場の工場内ネットワークの構成と運用〕

現在の K 工場の工場内ネットワークの構成を図 1 に，機器の概要を表 1 に示す。



FW: ファイアウォール

図 1　K 工場の工場内ネットワークの構成

表 1　K 工場の機器の概要（抜粋）

機器名	概要
製造統合管理サーバ	各種の製造装置を統合管理し，効率的な製造を実現するために使用する。
製造用 PC	製造統合管理サーバ又は製造装置と接続して，操作コンソールとして使用する。製造装置に設定ファイルを組み込む際にも使用する。
各種サーバ	プロキシサーバ，メールサーバ，ファイルサーバなどがあり，主に一般事務を行うために使用する。
事務用 PC	従業員が事務処理を行うために使用する。電子メールの送受信，プロキシサーバ経由でのインターネット上の Web サイトの閲覧が可能である。

製造装置へ組み込む設定ファイルが K 工場外から電子メールで送付される場合がある。製造用 PC では電子メールの利用が禁止されているので，設定ファイルは，事務用 PC で受信し，ファイルサーバ経由で製造用 PC へ転送している。

なお，PC やサーバには，ウイルス対策ソフトを導入するとともに，脆(ぜい)弱性修正プログラムの適用に努めている。脆弱性修正プログラムの適用に当たっては，事前に K

工場内で動作検証を行っており，開発元による提供が開始されてから適用されるまでには，1か月程度の日数を要している。

〔製造装置における脆弱性の問題〕

PC やサーバで広く利用されている汎用 OS が製造装置でも使用されるようになり，J 社が所属する業界団体において，汎用 OS の脆弱性が生産活動に与える影響が話題になっていた。そこで，K 工場では生産管理部が，製造装置の脆弱性について調査することになり，K 工場に設置している製造装置のうち，汎用 OS を使用している製造装置の脆弱性と対策について製造元に問合せを行った。その回答は，次のとおりであった。

・汎用 OS には特別なセキュリティ強化措置を施していない。
・製造装置は，汎用 OS の脆弱性を突く攻撃を受けた場合，影響や被害を受けるおそれがある。
・汎用 OS の脆弱性修正プログラムが提供された場合には，弊社（製造装置の製造元）で 3 か月掛けて動作確認試験を実施して問題がないことを確認している。それまでは適用後の製造装置の動作を保証できない。
・製造装置にウイルス対策ソフトを導入した場合には，リアルタイム応答性の低下が生じ得るので，製造装置の動作を保証できない。

〔製造装置における脆弱性への対策〕

当初，K 工場の生産管理部の R 部長は，製造装置は FW によって防御されているので，外部からの攻撃を受けることはなく，脆弱性への対処は不要だと考えていた。しかし，J 社内で情報セキュリティに関する管理を行っている情報システム課に相談したところ，次の指摘を受けて認識を新たにした。

・事務用 PC は，外部から電子メールを受信したり，インターネット上の Web サイトを閲覧したりするので，表 2 に示す感染方法をもつマルウェアに感染するおそれがある。さらに，これらのマルウェアがウイルス対策ソフトで検知されないこともある。
・事務用 PC 上のマルウェアによって，製造装置に被害が及ぶこともあり得る。

表２　製造装置に被害が及ぶと考えられるマルウェアの感染方法

マルウェアの型	感染方法
脆弱性攻撃型マルウェア	起動したマルウェアは，同一 LAN 上の他のコンピュータに対し，OS の脆弱性を悪用する攻撃を試み，攻撃に成功すると当該コンピュータを同マルウェアに感染させる。
ファイルばらまき型マルウェア	起動したマルウェアは，他のコンピュータ上で起動されることを期待して，同マルウェアに感染するような実行形式ファイルを共有ディスクや外部記憶媒体上に書き込む。

そこで，R 部長は生産管理部の P さんに対して，マルウェアによる製造装置への被害を防ぐために，事務用 PC が表 2 のマルウェアに感染した場合も考慮した上で，製造装置の脆弱性に関する対策を検討するよう指示した。併せて，検討に当たっては，情報システム課の支援を受けるよう指示した。P さんは，R 部長の指示に従って，次の(1)及び(2)を行った。

(1)　工場内 LAN を事務系 LAN と製造系 LAN に分離する構成見直し案（図 2）を作成し，さらに，二つの LAN の間のファイル転送方式案（表 3）を作成した。

(2)　図 2 と表 3 を情報システム課の Q 主任に提示し，助言を求めた。

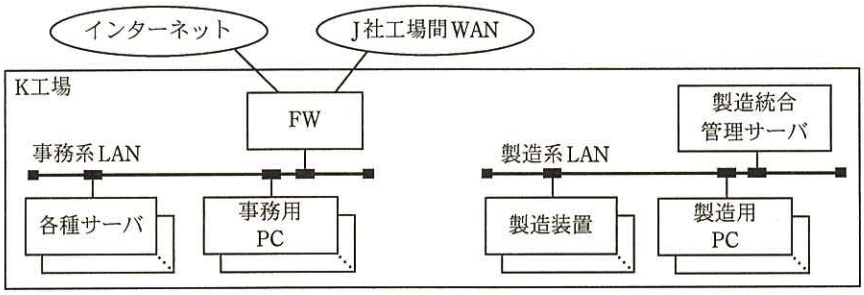
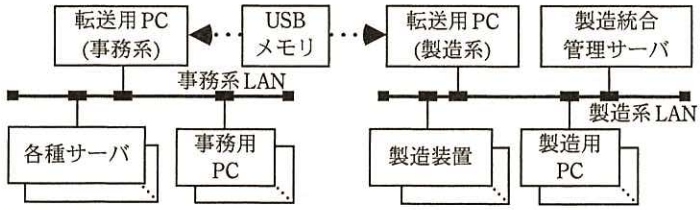
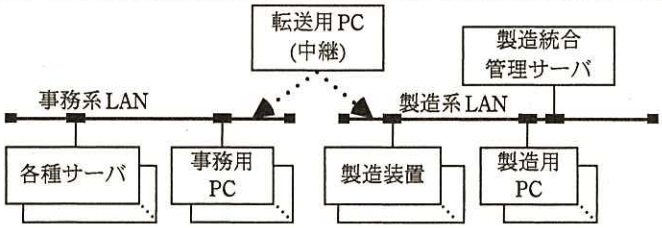


図２　工場内 LAN の構成見直し案

表3　ファイル転送方式案

名称	概要
USB メモリ方式	 ・ファイル転送に USB メモリを利用する。 ・転送元となる PC に USB メモリを接続して，ファイルを USB メモリに保存した後，転送先となる PC に USB メモリを接続して，製造装置などにファイルを転送する。
中継 PC 方式	 ・ファイル転送に転送用 PC を利用する。 ・転送元となる LAN に転送用 PC を接続して，ファイルを PC 内に保存した後，転送先となる LAN に物理的に接続を切り替えて製造装置などにファイルを転送する。

注記　FW，インターネット及び J 社工場間 WAN は，省略している。

Q 主任の見解は，次のとおりであった。

・製造装置を守るために，図 2 は有効な案である。

・表 3 のファイル転送方式案について安全性の評価をしたところ，結果は表 4 のようになった。

・USB メモリ方式を採用すべきである。ただし，実施に当たっては，転送用の USB メモリを限定し，かつ，他の用途に使用しないなど，適切な管理を行う必要がある。

表4　ファイル転送方式案の安全性の評価結果

名称	脆弱性攻撃型マルウェア	ファイルばらまき型マルウェア
USB メモリ方式	結論：製造装置への感染を防止できる。 理由：(省略)	結論：条件付きで，製造装置への感染を防止できる。 理由：マルウェアの複製が USB メモリに書き込まれることは防げないが，そのファイルを起動しないように徹底することによって，製造系 LAN 上の製造装置への感染を防止できる。
中継 PC 方式	結論：製造装置への感染を防止できない。 理由：[a]	結論：条件付きで，製造装置への感染を防止できる。 理由：マルウェアによって転送用 PC へファイルが書き込まれないように，ファイル共有機能を確実に停止することによって，製造系 LAN 上の製造装置への感染を防止できる。

Pさんは，図2の構成見直し案と，表3のうちのUSBメモリ方式をR部長に提案し，R部長はそれを承認した。

〔協力会社との情報共有〕

それから1年がたち，業界内の競争激化に伴い，K工場では多品種少量生産の効率向上が急務となった。K工場では，製造工程の一部を協力会社に委託しており，更なる生産効率の向上のためには，設計情報，K工場の稼働予定や製造実績などの情報を協力会社と共有する必要があると判断した。委託している工程には，表面加工，特殊溶接，出荷検査，こん包などがあり，現在の協力会社数は15社，各社の規模は従業員数30～200名である。

Pさんは，K工場と協力会社の間の情報のやり取りについて確認した。その結果，K工場から協力会社に提供する場合がほとんどであった。また，協力会社では，K工場の製造実績に応じて自社の製造装置の設定変更などの準備を行う必要があるので，製造実績の情報提供には即時性が求められることも分かった。

これらを受けて，生産管理部では，K工場から協力会社へ向けて情報を提供するために，情報共有サーバ（以下，Kサーバという）を構築することが決定された。設計・構築は，Pさんをリーダとしたチームで行うこととなった。またKサーバの運用も，生産管理部で行うこととなった。Kサーバで提供する情報は，表5のとおりである。

表5　Kサーバで提供する情報

名称	提供形式	概要	備考
設計情報	ダウンロード可能なファイル	工程の実施に必要な設計情報	協力会社が随時参照する。一部の設計情報は，設定ファイルとして協力会社の製造装置に組み込まれる。
稼働予定	Webページ	当日以降2週間のK工場の稼働予定	協力会社が稼働計画を立てるための元データとなる。
製造実績	Webページ	当日及び前日のK工場の製造実績	協力会社が稼働計画を調整するための元データとなる。

〔セキュリティポリシの確認〕

Pさんは，Kサーバの設計・構築に先立ち，J社のセキュリティポリシを確認した。J社のセキュリティポリシは，上位から順に，基本方針，対策基準及び実施規程の3

階層の文書で構成されている。そのうち，対策基準を図3に示す。

Ⅰ．適用範囲

本対策基準は，J社の情報資産を利用，管理又は閲覧する者（以下，取扱者という）及びJ社の情報資産の利用，管理又は閲覧に使用する機器（以下，情報機器という）に対して適用する。

Ⅱ．情報セキュリティ委員会の構成と役割

J社の情報セキュリティ管理体制における意思決定機関として，情報セキュリティ委員会を設ける。同委員会の委員長は，情報セキュリティ担当取締役とする。

（省略）

Ⅲ．情報資産の定義と分類

（省略）

Ⅳ．情報システムの構築と運用

1. 情報システムの審査

情報システムを構築する際には，構築に先立ち，当該情報システムにおけるセキュリティ要件及び実施規程について情報セキュリティ委員会の審査を受け，承認を得なければならない。また，情報システムの運用開始に先立ち，セキュリティ要件の実装状況について情報セキュリティ委員会の確認を受けなければならない。

2. 技術的基準

(1) 情報システムを構築する際には，次の情報セキュリティ対策の必要性を検討し，必要に応じて実装しなければならない。

・認証
・アクセス制御
・証跡管理
・情報機器における脆弱性対策
・情報機器における不正プログラム対策
・情報機器における情報漏えい対策
・ネットワークの分離・分割

(2) 情報システムを運用する際には，次の情報セキュリティ対策の必要性を検討し，必要に応じて実施しなければならない。

（省略）

Ⅴ．社外の取扱者及び社外の情報機器

J社の従業員ではない取扱者及びJ社の管理下にない情報機器について，J社が定める実施規程の遵守を求めるものとする。

（以下，省略）

図3　J社の対策基準

対策基準を確認したPさんは，Kサーバの審査に向けた準備を開始するとともに，Kサーバを利用する協力会社向けの実施規程案の作成に取り掛かった。作成に当たり，実施規程の対象者は，協力会社の情報システム部門のシステム管理者を想定した。Pさんは，Q主任の支援を受けながら実施規程案の作成を完了し，情報システム課の事前確認を受けた上で情報セキュリティ委員会に提出した。実施規程案のうち，Kサーバにアクセスするために利用するPC（以下，接続端末という）の管理に関する部分

を表6に示す。

表6　Kサーバを利用する協力会社向けの実施規程案（抜粋）

対策基準の項目	実施規程	
	小項目	内容
認証	利用者の限定と特定	Kサーバの利用に当たっては，許可された利用者以外の利用を防止するために，利用者の認証を必須とする。アカウントの共用は禁止する。
		マルウェアに感染する被害を低減するために，Kサーバを利用する際に接続端末にログインするためのアカウントは一般利用者権限とし，管理者権限を付与しない。
		他人による接続端末の利用を防止するために，利用者には，接続端末から離れる場合，［　b　］するように指導する。可能であれば，指導だけでなく強制する仕組みを整備する。
	パスワードの管理	パスワードは［　c　］ものを使用するよう指導するとともに，技術的に可能であれば，強制する仕組みを整備する。また，他人に［　d　］管理するよう指導する。
	接続端末の限定	Kサーバから取得した情報が漏えいする可能性を低減するために，Kサーバを利用する接続端末を限定する。
アクセス制御	ファイルへのアクセス制御	Kサーバからダウンロードしたファイルを保存する際には，必要最小限のアクセス権を付与する。
証跡管理	ログ取得設定	接続端末では，次の操作又は動作の際にログを取得するように設定する。 ・ログイン（失敗/成功問わず），ログアウト ・脆弱性修正プログラムの適用 ・マルウェアの検出
	ログの改ざん防止	一般利用者権限のアカウントには，ログの修正権限及び削除権限を付与しない。
	ログの消失防止	接続端末上のログ保存領域は，十分な容量を確保する。
		接続端末の管理者は，接続端末のログを定期的に収集して，磁気テープ，DVDなどの外部記憶媒体に保存する。
脆弱性対策	速やかな対策	接続端末に関する脆弱性が公表された場合には，速やかに［　e　］。

情報セキュリティ委員会では，この案について審査を行い，原案どおり承認し，実施規程として発行した。

〔Kサーバの設計・構築〕

Pさんをリーダとするチームでは，Kサーバの設計を次の(1)～(3)のとおりに進めた。

(1) 情報共有系 LAN の新設

P さんは設計作業の中で，K サーバを設置するために，新たに情報共有系 LAN を K 工場内に設けることにした。製造系 LAN に接続されている製造装置は，脆弱性の公表から対処までに時間が掛かることを念頭において，情報共有系 LAN の設計目標を次のように設定した。

・情報共有系 LAN には，K サーバと，K サーバを管理するための PC だけを設置する。

・情報共有系 LAN は，FW を経由してインターネットと接続する。

・情報共有系 LAN と製造系 LAN との間の一切の LAN 間通信を禁止するために，二つの LAN を分離する。FW を介した接続は分離とは認めない。

(2) K サーバで提供する情報の更新方法

提供する情報のうち，製造実績については，製造統合管理サーバが逐次作成する HTML ファイルを参照することにした。P さんは当初，この HTML ファイルの転送を，USB メモリ方式で実装しようと考えていた。しかし，製造実績に関するファイル転送の頻度を検討したところ，製造統合管理サーバから K サーバへのファイル転送が 1 時間に 10 回以上も行われることが想定されたので，USB メモリ方式で転送するのは現実的ではないと判断した。

そこで P さんは，製造統合管理サーバが FC（Fibre Channel）経由で使用している SAN（Storage Area Network）ストレージの機能である，ボリューム間の単方向レプリケーション機能に着目した。この機能を利用すると，ストレージ内のあるボリュームを他のボリュームに単方向コピーすることができる。P さんは，図 4 の構成を考え，K サーバが FC を経由して利用できる機能は，単方向レプリケーションによってコピーされたボリュームをマウントする機能だけとした。

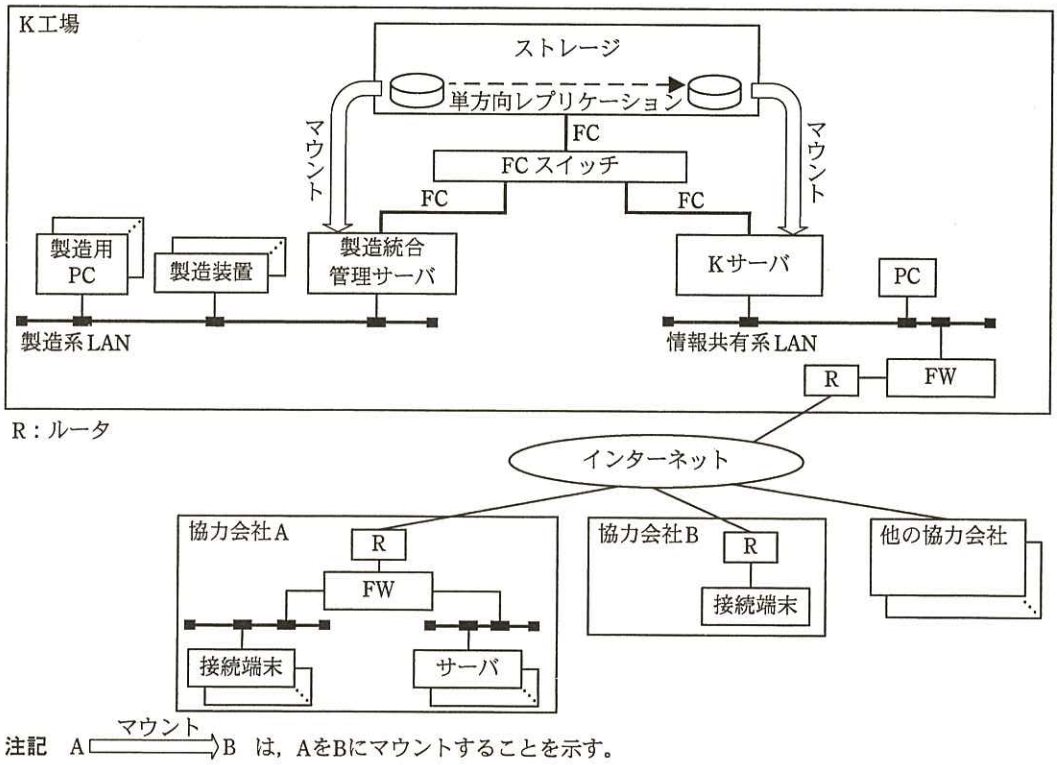


図４　Ｋサーバ及び関連機器の構成

(3)　協力会社からのアクセス方法

協力会社から K サーバへのアクセス方法及び協力会社でのネットワーク構成について，次の前提をおくことにした。

・K サーバを利用する各協力会社は，インターネットを利用して，社内の接続端末から K サーバへ HTTP over TLS を使用してアクセスする。

・K サーバの利用者には，利用者ごとに固有の利用者 ID を付与する。K サーバへのアクセス時に利用者 ID とパスワードで，K サーバの利用者を認証する。

・インターネットとの接続は，協力会社各社の既設設備を使用できるように，回線種別，固定 IP アドレスが割り当てられるか否かについて制限しない。

・協力会社内の LAN 構成については特に制限せず，プロキシサーバの有無及び NAT，NAPT の利用の有無にかかわらず利用できる。

〔K サーバ経由のマルウェア感染対策〕

P さんは図 4 の構成において，K サーバを経由した製造装置へのマルウェアの感染を防止できるかどうかを評価した。そのうち，協力会社の接続端末が表 2 のマルウェアに感染した場合に限定し，そのマルウェアが情報共有系 LAN まで到達したという状況を仮定した場合の評価結果は，表 7 のとおりである。

表 7　K サーバ及び関連機器の構成の安全性の評価結果（抜粋）

脆弱性攻撃型マルウェア	ファイルばらまき型マルウェア
結論：製造装置への感染を防止できる。 理由：［ f ］	結論：製造装置への感染を防止できる。 理由：［ g ］

〔K サーバを利用する接続端末の制限〕

P さんは，表 6 の実施規程において K サーバを利用する接続端末を限定するとしているものの，それを実現する技術的な仕組みがないことが気になっていた。そこで，K サーバにおいて接続端末を限定する仕組みについて，(1)～(4)の順に検討した。

(1)　アクセス元 IP アドレスによる端末認証の採用

実装が容易であることから，アクセス元の IP アドレスに基づく端末認証の仕組みを検討した。しかし，この仕組みでは，①実施規程に示された，K サーバを利用する接続端末の限定は実現できないことが分かった。

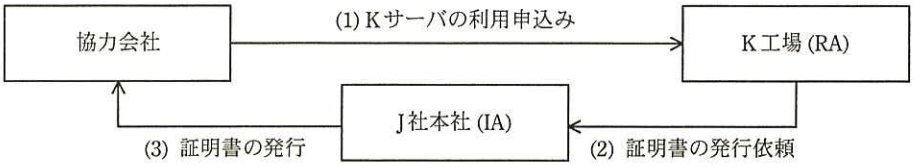
(2)　クライアント証明書による端末認証の採用

続いて，クライアント証明書（以下，証明書という）による端末認証の採用を検討した。この仕組みであれば，接続端末の限定が実現できると考えられたので，実装に向けた検討を続けた。

(3)　証明書の発行

証明書による端末認証を行う上で必須となる証明書の発行の流れを検討した。証明書の発行に必要な CA（認証局）の機能のうち，IA（発行局）については J 社本社のプライベート CA を利用し，RA（登録局）については K 工場が担当する。

なお，J 社本社のプライベート CA は，証明書発行業務を，一切，他に委任していない。また，J 社本社のプライベート CA は，中間 CA ではなく，ルート CA である。この分担に基づくと，証明書の発行の流れは，図 5 のようになる。



注記　それぞれ一意の識別名をもつ証明書を，接続端末ごとに発行する。

図5　証明書の発行の流れ

さらに，協力会社，K工場，J社本社の役割分担を表8のように定めた。

表8　証明書の発行及び利用に関する役割分担

役割	責任をもつ組織
鍵ペアの作成	K工場
証明書で証明するSubject（識別名）の一意性の確保	h
CSR（Certificate Signing Request）の発行	K工場
証明書の発行可否の判断	i
証明書の発行者としてディジタル署名の付与	j
接続端末への証明書のインストール	協力会社
Kサーバへアクセスしてきた接続端末が提示した証明書の有効性検証	k
CRL（Certificate Revocation List）の発行	ℓ

(4)　その他の手続の検討

証明書の発行以外に，更新及び失効についての手続を検討した。証明書の失効処理は，②協力会社がKサーバの利用を取りやめる申請をした場合以外にも行う必要があり，その点も考慮して手続を検討した。また，秘密鍵の機密性を保つために，協力会社へ周知すべき技術的事項を検討した。

その後，Kサーバの設計は順調に進み，情報セキュリティ委員会の審査を受け，許可を得た。引き続き構築作業を進め，構築完了後には実装状況の確認も終え，運用開始の日を迎えた。

設問1　表4中の［　a　］に入れる適切な記述を，マルウェアの感染方法を踏まえて，75字以内で具体的に述べよ。

設問2　〔セキュリティポリシの確認〕について，(1)，(2)に答えよ。

(1)　表6中の［　b　］～［　d　］に入れる適切な字句を，それぞれ10字以内で答えよ。

(2)　表6中の［　e　］に入れる適切な字句を，35字以内で具体的に述べよ。

設問3　表7中の［　f　］，［　g　］に入れる適切な理由を，［　f　］は40字以内で，［　g　］は60字以内でそれぞれ述べよ。

設問4　〔Kサーバを利用する接続端末の制限〕について，(1)～(4)に答えよ。

(1)　本文中の下線①について，アクセス元のIPアドレスでは接続端末が限定できないとPさんが考えた根拠を二つ挙げ，それぞれ50字以内で述べよ。

(2)　表8中の［　h　］～［　ℓ　］に入れる適切な組織を，協力会社，K工場，J社本社の中から選び，答えよ。

(3)　証明書の発行に当たっては，鍵ペアを利用する主体が鍵ペアを作成するのが原則であるが，接続端末用の証明書の発行の際は，K工場にて鍵ペアを作成している。K工場で作成してもよい理由を35字以内で述べよ。

(4)　本文中の下線②の場合以外に，失効処理が必要な場合を二つ挙げ，それぞれ30字以内で述べよ。