問1　公開鍵基盤の構築に関する次の記述を読んで，設問1～6に答えよ。

A社は，持株会社（以下，グループ本部という）を中心とした企業グループの中の一社であり，従業員数 1,200 名の中堅機械製造会社である。業務は，製造業向けの製造機械の製造である。A社には，製造部門以外に，人事総務部，商品管理部，営業部，配送部，情報システム部がある。商品管理部は，在庫管理が主な業務であり，受注状況によって，商品の製造指示を行っている。営業部は，販売推進とA社のグループ会社である販売会社（以下，グループ販社という）からの受注業務を行っている。受注業務には，電話とファックスを利用してきた。

グループ本部では，従業員のワークライフバランスに積極的に取り組んでおり，A社の経営者も，具体的な施策を段階的に実施してきている。ワークライフバランスへの取組の一環として，製造部門以外の部署を対象とするテレワーク環境（以下，Tシステムという）を提供することになった。

また，営業部における受注業務において，誤った商品の納品や，数量の誤りが年に数件発生し，損失と信用の失墜を招いていたので，受注誤りを減らすためのシステム（以下，Nシステムという）の構築もTシステム構築と同時に行うことになった。

両システムの構築は，情報システム部のX課長とZ主任が担当することになり，2人は検討を開始した。

〔Tシステムの検討〕

X課長とZ主任は，まず，Tシステムにおける，ネットワーク接続方法を検討した。次は，そのときの会話である。

X課長：まず，Tシステムの構築に当たって，利用形態や用途を洗い出し，どのようなネットワーク接続方法が適切かを考えてみよう。

Z主任：はい。最初にテレワークでの利用形態ですが，人事総務部のまとめによれば，現時点での対象者は，育児休職，介護休職を取得中で，在宅での勤務を希望する従業員です。その後，段階的に対象者の範囲を広げていくことになっています。勤務場所については，自宅以外にサテライトオフィスも検討されています。

X課長：作業の内容については，社内で行う作業のほとんどが対象となる。外部から無制限に社内のシステムにアクセスできることは，セキュリティ上の大きなリスクとなるから，何らかの制限をかける必要がある。どこから，どのシステムにアクセスする必要があるか，説明してくれ。

Z主任：はい。まず，場所ですが，従業員の自宅とサテライトオフィスからアクセスする必要があります。利用する社内システムには，二つの形態があります。一つは，Web システムの形態で，受注管理システム，発注管理システムとグループウェアがあります。もう一つは，クライアントサーバシステムの形態で，勤怠管理システムと電子メール（以下，メールという）があります。テレワークについての事前調査で，ほとんどの従業員は自宅でインターネットを利用できることが分かっています。サテライトオフィスについては，提供事業者に確認したところ，十分な帯域が確保されたインターネットが利用できるとのことでしたので，インターネットの利用を前提とすることは T システムの実現上，問題ないようです。

X課長：費用の面からも，公衆回線や専用線よりもインターネットを利用した方がよいだろう。インターネットを利用することになると，セキュリティ面での要件を検討する必要がある。

Z主任：そうですね。インターネットを利用することから，通信の盗聴や改ざんを防ぐことと，利用者を確実に認証することが必要になります。

X課長：それでは，当社のシステム構築を行っている C 社と相談して，T システムの通信はどのような仕組みにすべきか，検討してくれ。

Z主任：分かりました。

Z主任は，早速 C 社でセキュリティを担当している D 氏に連絡を取り，T システムにおける安全な通信方法について検討することにした。次は，そのときの会話である。

Z主任：T システムを，インターネットを利用して実現するために，IPsec を利用した VPN を構築したいと思いますが，どのようなことに注意する必要があるでしょうか。

D氏：テレワークで利用する PC（以下，テレワーク PC という）は，御社の社内ネ

ットワークに直接接続されるのと同様の状態になりますので，社内で使われているPC（以下，社内PCという）と同様の管理が必要になります。

Z主任：テレワークPCについては，社内PCと同じアプリケーションプログラム，ウイルス対策ソフトが導入されたものを貸与することにします。それでよろしいでしょうか。

D氏：それだけでは不十分です。例えば，御社では，ウイルス定義ファイルが，社内に設置されている配布用のサーバだけから自動的に配布されるようになっています。そのため，テレワークPCについては，①VPNで御社の社内ネットワークに接続されていないときに問題が起こる可能性がありますので，その対策が必要です。

D氏は，起こる可能性のある問題と，その対策方法について説明した。

Z主任：分かりました。対策を講じます。それから，不正な接続を防ぐために，信頼性の高い認証を行わなければならないと思いますが，どのような方法をとったらよいでしょうか。

D氏：利用者IDとパスワードによる認証ですと，総当たり攻撃などによって，正当な利用者以外の者が接続できてしまうリスクを無視できません。クライアント証明書を併用した認証方式を採用してはいかがでしょうか。

Z主任：そのようにしたいと思います。

数日後，Z主任はD氏との検討の結果を取りまとめ，D氏にも同席してもらい，X課長に報告した。

Z主任：Dさんと検討した結果，暗号化にはIPsec，認証にはクライアント証明書を利用することにしました。

X課長：分かった。運用上，秘密鍵とクライアント証明書の取扱いには注意が必要だ。そのことも考慮して，C社とともに作業に入ってくれ。

Z主任：そのように手配します。

X課長：ところで，現在広く使われている暗号方式には，暗号強度の問題や脆弱(ぜい)性の

問題がある，と聞いたことがあるのですが，どのようなことでしょうか。

D氏　：それは，米国国立標準技術研究所（NIST）が定めた，米国政府機関のコンピュータシステムの調達基準のことです。表に示す暗号アルゴリズムを利用したシステムなどの調達は2010年までしか認められていません。

表　米国政府調達基準で現在調達可能で
2011年以降調達できなくなる暗号アルゴリズム

分類	名称
共通鍵暗号	2-key Triple DES
公開鍵暗号	鍵長 [a] ビットの RSA 及び DSA 鍵長 160 ビットの ECDSA
ハッシュ関数	[b]

D氏　：この理由の一つは，コンピュータの性能が上がることによって，数年後には，現在広く利用されている，鍵長 [a] ビットの RSA 公開鍵から秘密鍵が推測される可能性があり，②電子署名の対象のデータの改ざんやなりすましが行われる可能性があることです。これに対しては，鍵長を更に長くすることが求められます。もう一つは，ハッシュ関数として現在広く利用されている [b] には，ある条件下で [c] の衝突を意図的に起こすことができる，という脆弱性が発見されていることです。この脆弱性を攻撃されると，電子署名の信頼性が損なわれます。

X課長：なるほど。表の暗号アルゴリズムの問題には今から対策を講じておく必要があるわけですね。

D氏　：はい。日本でも政府機関に対して，内閣官房情報セキュリティセンターが2013年度までに対応するように求めています。

X課長：これらは政府機関の基準だが，我々のような民間企業でも，暗号アルゴリズムの問題を考慮してシステムを構築した方がよさそうですね。

D氏　：新規に構築するシステムですので，暗号アルゴリズムの問題を考慮した方がよいと考えます。

X課長：Z主任，この件についても，要求仕様を作る上で，十分に気をつけてくれ。

Z主任：はい，分かりました。

〔N システム要件の検討〕

続いて，X 課長と Z 主任は，受注誤りへの対応を行うために，営業部の Y 主任を交えて，N システムの要件を洗い出すことにした。次は，そのときの会話である。

X 課長：これまでの電話とファックスによる受注が，どのようなフローで行われているかを確認しよう。Y 主任，説明してくれ。

Y 主任：はい。まず，電話による受注処理ですが，営業部の従業員が電話を受け，その内容を注文票に記入します。注文票の内容を，同じ従業員が，社内システムの受注管理システムに入力します。商品管理部は，受注管理システムを参照して在庫情報を確認し，製造指示作業を始めます。次に，ファックスによる受注処理ですが，営業部の従業員が，受け取ったファックスの内容を，受注管理システムに入力するようになっています。以後は電話による受注処理と同じです。

X 課長：どのような受注誤りが多いのかね。

Y 主任：受注誤りで多いのは，受注管理システムへの型番や数量の入力間違いです。

X 課長：それでは，表計算ソフトを使って電子化した注文票を，送付してもらってはどうだろうか。そうすれば，受注管理システムとの連携は，比較的容易に構築できるだろう。

Z 主任：注文票には，グループ販社の担当者の氏名や電話番号，お客様の事業状況などがうかがい知れる項目が含まれていますので，グループ販社の発注担当者と当社営業部担当者間の機密性を確保することが必要です。

X 課長：それでは，電子化された注文票の送付方法について検討することにしよう。

電子化された注文票を安全に送付する方法について，再び，D 氏に相談することにした。次は，そのときの会話である。

X 課長：電子化された注文票は，注文票を作成したグループ販社と当社の者だけが，内容を知ることができるようにしたいと考えています。電子化された注文票を，インターネットを使って安全に送付する方法として，どのようなものがあるか教えてほしいのですが。

D氏　：送付する方法としては，メールを利用する方法と，Web システムを利用する方法があります。どちらの方法でも，暗号化を利用すれば，安全に送付することができます。

Z主任：Web システムを利用する場合は，SSL で暗号化された通信路を使って送付することになりますよね。メールを利用する場合は，どのような方法で行うのですか。

D氏　：はい，S/MIME という方法があります。これは，RFC で規定されており，多くのメールソフトが標準で実装しています。S/MIME を使うと，メールの暗号化と電子署名を行うことができます。

SSL も S/MIME も公開鍵基盤（PKI）の上で動作しますので，まず，認証局（CA）が必要となります。これには，認証事業者の CA（以下，商用 CA という）を利用することもできますし，御社で構築，運用する CA（以下，自営 CA という）を利用することもできます。利用者は，自分自身の秘密鍵と公開鍵の対（以下，鍵ペアという）を生成します。CA は，この公開鍵に対して公開鍵証明書（以下，証明書という）を発行します。御社での CA の設置運用状況は，どうなっていますか。

X課長：はい，グループ本部では，既に証明書ポリシと認証局運用規程（以下，CP/CPS という）を策定しており，ルート CA が自営 CA として設置されています。グループ企業はこのルート CA の利用が可能です。また，グループ企業独自のルート CA を設置してもよいことになっており，商用 CA と自営 CA のいずれで実現しても構わないことになっています。

Z主任：今回の場合，証明書の発行をタイムリに行う必要があると思うので，独自のルート CA を設置した方がよいと思います。

X課長：そうだな。グループ本部のルート CA を利用するのではなく，当社独自のルート CA を設置することにしよう。

D氏　：分かりました。

X課長：この場合，商用 CA を利用するか，自営 CA を利用するかは何を基準にして決めればよいのですか。

D氏　：まず，だれが証明書を利用するのかが基準になります。不特定の利用者を対象とする場合は，商用 CA を利用しなければなりませんが，利用者の範囲が

限られる場合は，自営 CA を利用しても構いません。次に，自営 CA の構築費用及び証明書発行費用を含む運用費用と，商用 CA の費用との比較によって決めるのが一般的です。

Z主任 ：今回の場合，利用者がグループ販社と当社に限定されるので，利用者の範囲という観点では，自営 CA でも問題なさそうですね。後は，費用と手間の観点での検討が必要ということですね。自営 CA を運用する場合，どのようなことをしないといけないのでしょうか。

D氏 ：構築段階では，自営 CA で発行する証明書の種類を決めたり，証明書発行の手順や運用体制を決めたりしなければなりません。これらを文書化して CP/CPS を策定する必要があります。運用段階の主な作業は，証明書の発行と証明書失効リストの発行です。

X課長：自営 CA の構築はどのように行うのでしょうか。

D氏 ：自営 CA を構築する方法は幾つかあります。一つ目は，OS の機能やオープンソースソフトウェア（OSS）を使う方法です。二つ目は，アプライアンス製品を使う方法です。三つ目は，市販されている CA ソフトを使う方法です。

Z主任 ：OSS を利用すると，構築費用はかなり下げることができますね。ただし，そのソフトウェアに精通した技術者が必要になると思いますが。

X課長：そうだな。Z 主任，これらの情報を基に，電子化された注文票の送付方法をメールと Web システムのどちらにするか，CA は自営 CA と商用 CA のどちらにするか，また，自営 CA を利用する場合は，CA の構築方法も含めて検討してくれ。

Z主任 ：分かりました。

〔PKI 構築の検討〕

数日後，X 課長は，Z 主任の検討結果が適切であるかを，D 氏を交えて確認した。

Z主任 ：電子化された注文票の送付方法について検討したところ，Web システムを利用した送付については，Web システムの開発が必要ですので，すぐには開始できません。メールについては，証明書が用意できれば，すぐにでも開始できます。受注管理システムとの連携をスムーズに行うために，将来的には

Web システムを利用することにして，しばらくの間は，メールにすることにしました。

X課長：そうか。CAについてはどうかね。

Z主任：T システムと N システムを合わせると，発行する証明書がかなりの数になります。そのため，多数の証明書を一括して発行できる証明書発行プログラムが必要になりますので，その開発費用も含め，3 年間で掛かる総費用を算出してみました。なお，CP/CPS については，グループ本部の CP/CPS を流用することができますので，比較的容易に策定することができます。その結果，当社にとって最適な方式を採用した自営 CA を利用する場合が 359 万円，商用 CA を利用する場合が 654 万円となり，当社の場合，自営 CA を利用した方が安いとの結論に至りました。

D氏　：なるほど。しかし，証明書を発行するために，自営 CA の秘密鍵を使う必要があります。③自営 CA の秘密鍵が漏えいすると，グループ販社と御社に被害が及ぶことが想定されます。秘密鍵の漏えい防止対策を施すと，証明書発行に要する費用は，これよりは多くなると思います。

X課長：そのとおりだ。自営 CA の秘密鍵を安全に使うための手順を考慮して，証明書発行に要する費用を再度計算してくれ。

Z主任：分かりました。

Z主任は，自営CAの秘密鍵を安全に使うための手順を考慮した費用を計算し，X課長に提示した。

Z主任：秘密鍵を安全に使うための手順を見直したところ，鍵管理のアプライアンス製品を導入することで，秘密鍵を安全に管理できることが分かりました。この製品を使用した場合の 3 年間の総費用は 422 万円となり，やはり，自営CAを利用する方が安くなります。

X課長：それでは，自営 CA を利用することにしよう。Web システムになったとしてもCAは必要だからな。

Z主任：分かりました。ところで，利用者が証明書署名要求（CSR）を作成するためには，事前に，鍵ペアを生成しておく必要があります。また，CA で証明書

発行を行うためには，利用者からCSRをもらう必要があります。

X課長：証明書発行プログラムとは別に，鍵ペアの生成プログラムと，CSR 作成プログラムの開発が必要ということだな。ただ，今回の場合，証明書を T システムと N システムの利用に限定すれば，必ずしも CSR の作成までを，利用者に行ってもらう必要はないのではないでしょうか。

D氏　：おっしゃるとおりです。今回の PKI 構築の目的は，御社とグループ販社の担当者間のメールを，第三者が不正に閲覧することができなければよいわけですから，必ずしも，鍵ペアを利用者本人が生成しなくても，御社が生成すれば問題ないと考えます。鍵ペアを御社が生成するのであれば，CSR 作成も御社で可能です。鍵ペアの生成プログラムと CSR 作成プログラムは，証明書発行プログラムの一部として開発すれば，運用も容易になると思います。

X課長：そういうことだ。この方法を採用する方がよさそうだな。ただし，CP/CPSの中で，④利用者の鍵ペアの取扱いについて，きちんと決めておいた方がよさそうだ。Z 主任，D 氏とともに，テレワークを含め，証明書発行の運用フロー概要を作成してくれたまえ。

Z主任：分かりました。

翌日，Z主任は，証明書発行の運用フローをX課長に提示した。

Z主任：証明書発行の運用フローを，図 1 にまとめました。T システムで利用する証明書と，N システムで利用する証明書のいずれも，同じ CA で発行するようにしています。また，鍵ペアの生成及び CSR の作成は CA 運用者で行う方法を採用しています。

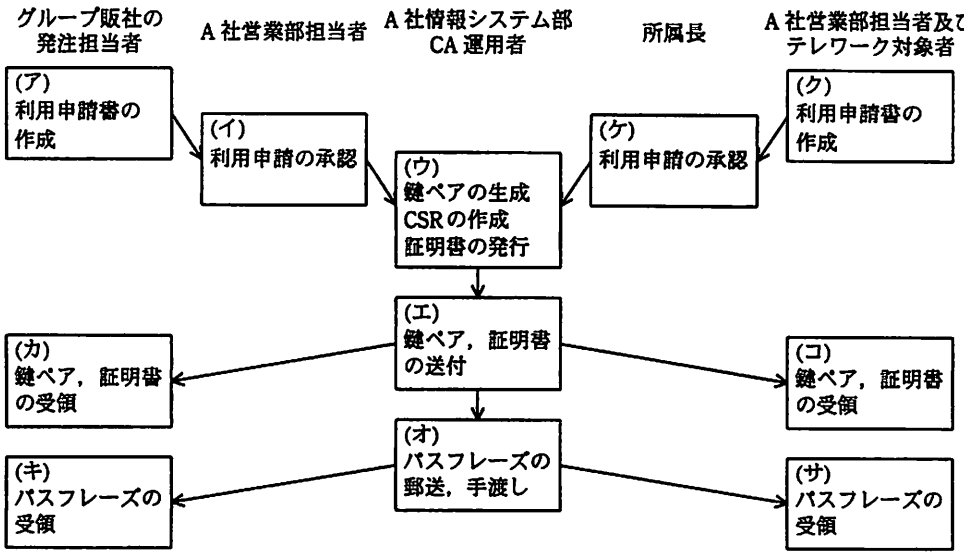

図１　証明書発行の運用フロー

X課長：ところで，利用者属性の真偽の確認は，どこで行うのかね。

Z主任：グループ販社の発注担当者の確認は，図１中の［　d　］で行います。テレワーク対象者の確認は［　e　］で行います。

X課長：登録局（RA）の役割を，利用申請者をよく知っている当社の従業員が担う形になるわけだな。鍵ペアと証明書は，利用申請者にどのような手段で渡すのかね。

Z主任：鍵ペアと証明書は，パスフレーズを使って暗号化し，メールで送付します。復号に必要なパスフレーズは，グループ販社の場合は郵送します。当社営業部担当者とテレワーク対象者の場合は，情報システム部に取りに来てもらいます。

X課長：分かった。ところで，実際の受注フローについては，どのようになるのかね。

Z主任：はい，図２にまとめました。

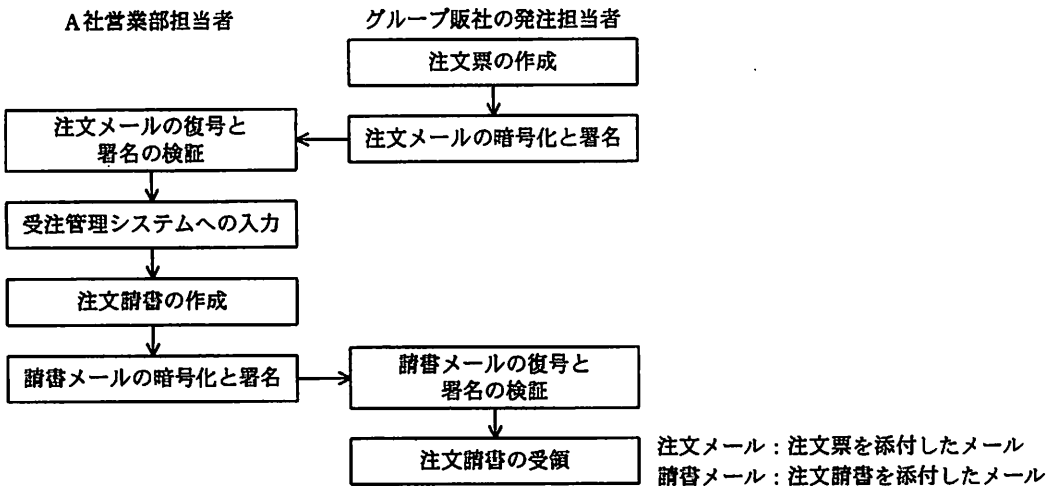

図２　受注フロー

X課長：グループ販社側で，注文メールの暗号化と署名，請書メールの復号と署名の検証に手間が掛かるが，最近のメールソフトでは，簡単な操作でこれらができるようになっているから，グループ販社にとっても，そんなに面倒な作業ではないだろう。受注管理システムへの入力は，注文票に組み込まれているプログラムで自動化することで，誤りが防げる。

ところで，当社営業部担当者の証明書をグループ販社の発注担当者に送っておく必要があるが，どのようにするのかね。それから，グループ販社と当社ともに，メールの暗号化と署名の検証を行う必要がある。そのときに必要となる当社の［ f ］証明書は，いつ，どこに，どのようにして導入するかを手順書として整備する必要があるな。

Z主任：すみません，それらのことを忘れていました。当社営業部担当者の証明書の送付方法と［ f ］証明書の導入については，手順書を作成して配布するようにします。また，グループ販社での導入を支援できるように，営業部員への教育を検討します。

X課長：CP/CPS についても，営業部員がきちんと説明できるようにしておいてくれ。それから，⑤グループ販社では，証明書を N システム以外の用途に使用しないように，徹底してくれ。

Z主任：分かりました。

その後，X課長とZ主任は，C社とともにTシステムとNシステムの構築を順調に終え，運用を開始した。

設問1　本文中の［　a　］～［　c　］及び［　f　］に入れる適切な字句を，8字以内で答えよ。

設問2　本文中の下線①について，どのような問題が起こるかを，45字以内で述べよ。また，その対策を，50字以内で述べよ。

設問3　Tシステムにおいて，テレワーク対象者は，他人が社内ネットワークへ不正にアクセスしないようにするために，自分のテレワークPCに関して，運用する上でどのような点に注意する必要があるか。秘密鍵の漏えい防止の観点から二つ挙げ，それぞれ35字以内で述べよ。

設問4　本文中の下線②について，秘密鍵の推測が成功したとして，どのようにすれば改ざんやなりすましができるか。その方法を，70字以内で述べよ。

設問5　PKI構築について，(1)～(3)に答えよ。

(1) 本文中の下線③について，どのような被害が考えられるか。50字以内で述べよ。

(2) 本文中の［　d　］と［　e　］に入れる適切な記号を，図1中の(ア)～(サ)から選んで答えよ。

(3) 本文中の下線④について，鍵ペアの取扱い上で注意すべき事項を，30字以内で述べよ。

設問6　本文中の下線⑤について，グループ販社の発注担当者が，証明書の使用制限に反して，第三者に対し，A社の自営CAで生成された秘密鍵を用いて署名したメールを送付した場合，メール受信者では，どのような問題が発生するか。また，その理由は何か。A社が自営CAを採用していることを考慮して，それぞれ20字以内，30字以内で述べよ。