SC

平成27年度　春期
情報セキュリティスペシャリスト試験
午後Ⅱ　問題

試験時間	14:30 ～ 16:30（2時間）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. **答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。**
4. 問題は，次の表に従って解答してください。

問題番号	問1，問2
選択方法	1問選択

5. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) B又はHBの黒鉛筆又はシャープペンシルを使用してください。
   (2) **受験番号欄**に**受験番号**を，**生年月日欄**に**受験票の生年月日**を記入してください。正しく記入されていない場合は，採点されないことがあります。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入してください。
   (3) **選択した問題**については，次の例に従って，**選択欄**の**問題番号**を○印で囲んでください。○印がない場合は，採点されません。2問とも○印で囲んだ場合は，はじめの1問について採点します。
   (4) 解答は，問題番号ごとに指定された枠内に記入してください。
   (5) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

〔問2を選択した場合の例〕

選択欄	
1問選択	問1
	(問2)

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

問1　ウイルス対策に関する次の記述を読んで，設問1～6に答えよ。

N社は，従業員数500名のシステム開発会社である。東京の本社には，管理本部と東日本ソリューション本部（以下，東ソリ本部という）がある。管理本部には，業務部，総務部，営業部及び情報システム部（以下，情シス部という）がある。大阪の関西支社には，西日本ソリューション本部（以下，西ソリ本部という）があり，100名が在籍している。

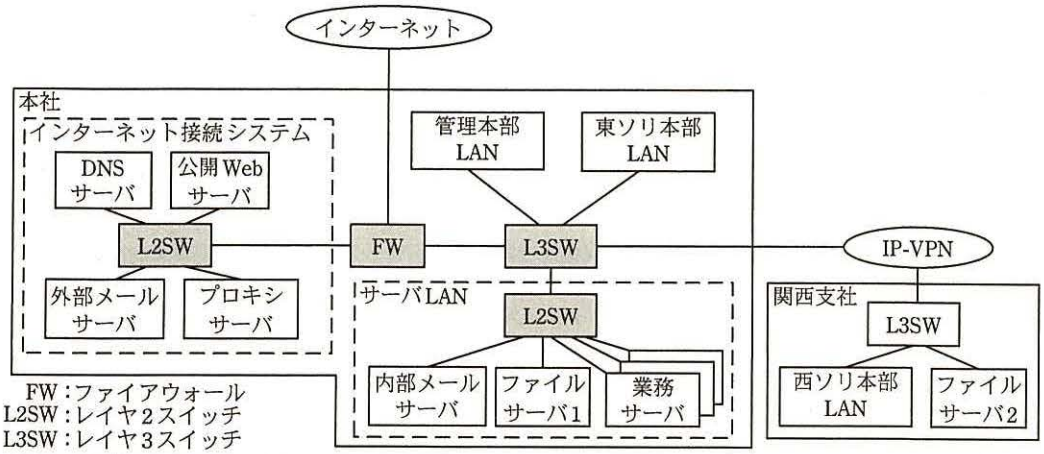
N社では，本社にインターネット接続システムを導入し，電子メール（以下，メールという），Webサイトの閲覧などに利用している。ドメイン名としてn-sha.co.jpを使用しており，メールアドレスには，表1に示すものがある。

表1　N社のメールアドレスと概要

種別		メールアドレス	概要
従業員用メールアドレス		*user*@n-sha.co.jp	従業員が利用するメールアドレスである。*user*は，従業員ごとに異なる文字列を割り当てる。
管理用メールアドレス	採用問合せ用メールアドレス	saiyou@n-sha.co.jp	採用に関する問合せメールを受信したり，回答メールを送信したりするメールアドレスである。このメールアドレス宛てに届いたメールは，総務部採用グループのメンバのメールアドレス宛てに同報される。
	広報問合せ用メールアドレス	kouhou@n-sha.co.jp	広報に関する問合せメールを受信したり，回答メールを送信したりするメールアドレスである。このメールアドレス宛てに届いたメールは，営業部広報グループのメンバのメールアドレス宛てに同報される。
	運用グループ用メールアドレス	postmaster@n-sha.co.jp	配送不能通知（Non-Delivery Report）メールを送受信したり，運用に関するメールを受信したりするメールアドレスである。このメールアドレス宛てに届いたメールは，情シス部運用グループのメンバのメールアドレス宛てに同報される。

〔情報システムの構成〕

N社の情報システムの運用は，情シス部のD部長の下で，運用グループのメンバが担当している。N社の情報システムのネットワーク構成を図1に，主な機器の概要を表2に示す。



注記1　網掛けの機器は二重化している。

注記2　PCは全て，管理本部LAN，東ソリ本部LAN及び西ソリ本部LANのいずれかに接続している。

注記3　PCの記載は省略している。

図1　N社の情報システムのネットワーク構成

表2　主な機器の概要

機器名	概要
FW	・ステートフルパケットインスペクション型のパケットフィルタリング機能，アドレス変換機能並びに通信の許可及び拒否のログを取得する機能がある。
DNSサーバ	・DNS機能及びNTPサーバ機能がある。 ・DNS機能では，DNSの拡張仕様である［　a　］を用いた，公開鍵暗号方式によるディジタル署名のDNSレコードへの付加と，DNS応答のディジタル署名の検証が可能である。また，インターネットからの再帰的な名前解決問合せを拒否することによって，このDNSサーバが，［　b　］リゾルバとして踏み台にされないようにしている。 ・NTPサーバ機能は，インターネット上のNTPサーバと時刻同期している。さらに，FW，公開Webサーバ，外部メールサーバ，プロキシサーバ及び内部メールサーバは，DNSサーバと時刻同期している。
公開Webサーバ	・コンテンツ公開機能及びコンテンツ更新機能がある。コンテンツ更新は，営業部広報グループのメンバがPCからSSHを用いて行う。
外部メールサーバ	・インターネットと内部メールサーバとの間のメール転送機能がある。メール転送機能では，SMTPの［　c　］中の宛先情報を用いた不正中継防止設定が可能である。不正中継防止設定をすることによって，外部メールサーバは宛先メールアドレスのドメイン名が［　d　］であるメールは内部メールサーバに転送し，それ以外のメールは拒否する。

表2　主な機器の概要（続き）

機器名	概要
プロキシサーバ	・インターネットへのHTTP及びHTTP over TLSによるWebアクセス中継機能，Webコンテンツキャッシュ機能，HTTPに対応したウイルススキャン（以下，HTTPウイルススキャンという）機能及びURLフィルタリング機能がある。 ・Webコンテンツキャッシュ機能では，Webサーバごとにキャッシュの要否を設定できる。 ・URLフィルタリング機能では，ネットワークを送信元として指定したフィルタリングルールを作成することができる。フィルタリングルールには，適用順に，サーバ管理者登録ホワイトリスト，サーバ管理者登録ブラックリスト及びベンダ提供ブラックリストがあり，最初に一致したフィルタリングルールが適用される。サーバ管理者登録ホワイトリスト及びサーバ管理者登録ブラックリストには，パターンマッチングの方式と文字列を登録できる。パターンマッチングの方式には，完全一致，部分一致，前方一致又は後方一致のいずれかを指定する。 N社では，サーバ管理者登録ブラックリストとベンダ提供ブラックリストを使用している。
内部メールサーバ	・外部メールサーバとの間のメール転送機能，SMTPに対応したウイルススキャン（以下，SMTPウイルススキャンという）機能，PCとの間のメール送受信機能，及びNTPサーバ機能がある。ファイルサーバ1，ファイルサーバ2，業務サーバ及びPCは内部メールサーバと時刻同期している。
ファイルサーバ1，ファイルサーバ2	・システム開発プロジェクト用のデータを保存する。DHCPサーバ機能がある。
業務サーバ	・社内通達，人事情報，経理情報，営業情報などを格納する。Webインタフェースでアクセスする。FTPを利用してコンテンツの更新や管理を行う。

FW，L2SW，L3SW及び各サーバは，保守時を除き24時間365日稼働している。

FWでは，通信の許可及び拒否のログを取得している。各サーバでは，サーバへのアクセス及びサーバ上でのプログラムの動作をログに記録している。FW及び各サーバのログの保存期間は，6か月である。

PCのIPアドレスは，L3SWのDHCPリレーエージェント機能によって動的に割り当てている。

〔ウイルス対策〕

N社では，HTTPウイルススキャン及びSMTPウイルススキャンにはV社のウイルス対策ソフトを導入し，ファイルサーバ1，ファイルサーバ2，業務サーバ及びPCにはW社のウイルス対策ソフトを導入している。2社のウイルス対策ソフトを導入することによって，1社の場合よりも早くウイルスを検出できるようになると期待されている。

サーバ及びPCに関するN社のウイルス対策の概要を表3に示す。

表3　サーバ及びPCに関するN社のウイルス対策の概要

機器名	概要
プロキシサーバ	・ウイルス定義ファイルは，1時間ごとにV社のWebサーバからダウンロードし，更新する。 ・PC及び他のサーバが最新のウイルス定義ファイルをダウンロードできるように，V社及びW社のWebサーバのコンテンツはキャッシュしない設定にしている。 ・HTTP ウイルススキャン機能では，結果を Web ブラウザへの表示やメールによって，通知することができる。
内部メールサーバ	・ウイルス定義ファイルは，1時間ごとにプロキシサーバ経由でV社のWebサーバからダウンロードし，更新する。 ・SMTP ウイルススキャン機能では，結果をメールで通知することができる。
ファイルサーバ1， ファイルサーバ2， 業務サーバ	・ウイルス定義ファイルは，1時間ごとにプロキシサーバ経由で W 社の Web サーバからダウンロードし，更新する。 ・ファイルの読み書き時にリアルタイムスキャンを行う。 ・毎週，日曜日の2時に全てのファイルのウイルススキャン（以下，フルスキャンという）を開始する。
PC	・ウイルス定義ファイルは，起動時及び起動後1時間ごとにプロキシサーバ経由でW社の Web サーバからダウンロードし，更新する。ウイルス定義ファイルのダウンロードと更新は手動でも実行できる。 ・ファイルの読み書き時にリアルタイムスキャンを行う。 ・毎週，月曜日の昼の 12 時にフルスキャンを開始する。フルスキャンは手動でも実行できる。 ・ウイルス定義ファイルの未更新期間が1週間以上の場合は，ウイルス定義ファイル全体をダウンロードする。ダウンロードするファイルの大きさは，300 M バイト以上となる。未更新期間が1週間未満の場合は，リリースされているウイルス定義ファイルのうち，未更新の情報だけをダウンロードする。ダウンロードするファイルの大きさは，通常 20 M バイト以下である。

長期の休み明けの始業時には，N社の全PCが一斉にウイルス定義ファイル全体をダウンロードするので，インターネット回線及びIP-VPNが一時的に輻輳（ふくそう）する。その解決が課題になっている。

HTTP ウイルススキャンの結果と通知方法を図2に，SMTP ウイルススキャンの結果と通知方法を図3に示す。

(1) 結果
HTTP ウイルススキャンでは，ファイルがウイルススキャンできるかどうかを判定する。もし，ウイルススキャンができる状態であれば，ウイルススキャンを行う。例えば，暗号化されたファイルは，ウイルススキャンができない状態（以下，スキャン不能という）と判定される。判定結果は，次のいずれかである。
・検出
・不検出
・スキャン不能
検出の場合は，ダウンロードを中止し，結果をログに記録する。
(2) 結果の通知条件及び通知方法
検出の場合は，結果を次の方法で通知する。
・利用者の PC の Web ブラウザへの表示
・運用グループ用メールアドレス宛ての通知メールの送信
不検出及びスキャン不能の場合は，結果を通知しない設定としている。

図 2　HTTP ウイルススキャンの結果と通知方法

(1) 結果
SMTP ウイルススキャンでは，メールがウイルススキャンできるかどうかを判定する。もし，ウイルススキャンができる状態であれば，ウイルススキャンを行う。例えば，暗号化されたファイルは，スキャン不能と判定される。判定結果は，次のいずれかである。
・検出
・不検出
・スキャン不能
検出の場合は，メールを破棄し，結果をログに記録する。
(2) 結果の通知条件及び通知方法
検出の場合は，結果を次の方法で通知する。
・次のメールアドレス宛ての，ウイルススキャンしたメールのヘッダ部を添付した通知メールの送信
- 運用グループ用メールアドレス
- PC から送信されたメールの場合，送信者メールアドレス
- 外部メールサーバから転送されたメールの場合，宛先のメールアドレス
ここで，［　e　］に送信するのではなく，宛先のメールアドレスに送信するのは，［　e　］に通知メールを送信すると迷惑メールになる可能性があるからである。
不検出及びスキャン不能の場合は，結果を通知しない設定としている。

図 3　SMTP ウイルススキャンの結果と通知方法

〔PC の管理方法〕

従業員には，PC を会社から貸与している。従業員は，出勤後に個人ロッカーから PC を取り出して使用し，退勤前に，PC を個人ロッカーにしまう。個人ロッカーは，施錠を必須としている。

PC の初期設定は，情シス部が担当し，OS，ウイルス対策ソフトなど N 社で定めたソフトウェアのインストール，脆弱(ぜいじゃく)性修正プログラムの適用，ウイルス定義ファイルの更新，Web ブラウザの設定及びメールソフトの設定を行う。その際には，脆

弱性修正プログラム及びウイルス定義ファイルを保存した DVD-R（以下，初期設定用 DVD-R という）を使用している。初期設定用 DVD-R は月 1 回，新しいものを作成する。

脆弱性修正プログラムの適用順序を確認したり，ウイルス定義ファイルをダウンロードしたりするのに時間が掛かるので，初期設定用 DVD-R 作成の作業負荷は大きく，効率向上が課題となっている。

そこで，運用グループの E 主任と F さんが，PC の初期設定方法の改善を検討することになった。

〔PC の初期設定方法の改善〕

PC の初期設定方法を改善するために F さんが作成した初期設定用ネットワークの設置案を図 4 に示す。

1. ネットワーク構成の改善
(1) 初期設定用ネットワークの設置
本社に，初期設定用ネットワークを設置する。
(2) FW の導入
FW 機能があるブロードバンドルータ（以下，初期設定用 FW という）を導入する。
(3) 初期設定用ネットワークの接続
初期設定用ネットワークを，初期設定用 FW を介して本社の L3SW と接続する。

図 4　初期設定用ネットワークの設置案（抜粋）

初期設定用 FW のフィルタリングルールを表 4 に示す。

表 4　初期設定用 FW のフィルタリングルール

項番	送信元	宛先	サービス	動作	ログ
1	初期設定用ネットワーク	プロキシサーバ	代替 HTTP	許可	取得する
2	全て	全て	全て	拒否	取得しない

注記 1　項番が小さいルールから順に，最初に一致したルールが適用される。
注記 2　代替 HTTP のポート番号は，8080 である。

E 主任は，PC の初期設定方法を考慮すると，プロキシサーバの URL フィルタリング機能に，①初期設定用ネットワークからの接続サイトを制限する設定を追加した方がよいと指摘した。F さんは，その設定案を作成して E 主任に提出した。

初期設定方法の改善案は，D 部長の承認を得られた。F さんは，プロキシサーバの URL フィルタリング機能に設定を追加した後，初期設定用 FW を介して本社の L3SW と初期設定用ネットワークを接続した。

〔休み明けの PC のウイルス感染〕

N 社では 4 月 29 日から 5 月 6 日まで連休であった。連休明けの最初の営業日となった 5 月 7 日，D 部長に，“広報グループの G さんの PC がウイルスに感染した可能性があり，ネットワークから切り離した”との連絡があった。D 部長は，E 主任と F さんに調査と対処を指示した。F さんの調査結果と感染への対処を図 5 に示す。

(1) G さんへのヒアリング結果
- 4 月 28 日 18 時，業務を終了し，PC を個人ロッカーにしまった。
- 5 月 7 日 8 時 40 分，PC を個人ロッカーから取り出し，管理本部 LAN に接続し，起動した。
- 5 月 7 日 8 時 45 分，PC 上のメールソフトにメールを受信した。
- 5 月 7 日 9 時 30 分，広報問合せ用メールアドレス宛てのメールを開いた。そのメールには，パスワードを用いて暗号化されたファイルが添付されており，別のメールに書かれていたパスワードを使用してその添付ファイルを開いた。
- 5 月 7 日 11 時，同じ添付ファイルを開くと，PC のウイルス対策ソフトが，マルウェア X を検出した。

(2) マルウェア X に関する情報
- 調査の時点では，W 社の Web サイトに，マルウェア X に関する次の情報が掲載されていた。
  - ダウンローダ型マルウェアであり，マルウェア X 中に URL が保持されている。
  - マルウェア X 中の URL にアクセスすると，中継サーバと呼ばれるインターネット上のサーバを経由して，攻撃者がインターネット上に用意した C&C（Command & Control）サーバに接続される。
    マルウェア X 中の URL の例を次に示す。
    http://www.example.com.server.example.net/cmd/command.html
  - 上記 URL 中の中継サーバ名を次に示す。
    server.example.net
    マルウェア X 中の URL にアクセスすると，中継サーバが，攻撃者の用意した C&C サーバに次の URL で接続する。
    http://www.example.com/cmd/command.html
  - W 社の駆除ツールを適用すると，マルウェア X を駆除し，感染によって改ざんされた OS の設定を復元する。
  - 駆除ツールは，W 社の Web サーバからダウンロードできる。

(3) G さんの PC に関するウイルス対策ソフトの調査
- 5 月 3 日 10 時，W 社では，マルウェア X に対応したウイルス定義ファイルをリリースした。
- 5 月 7 日 10 時 40 分，全てのウイルス定義ファイルをダウンロードし，更新した。

(4) 対処
- G さんの PC を預かり，他の PC やサーバへのネットワークを経由した感染を防ぐために，②先頃，改善された N 社の環境を活用し，マルウェア X を駆除した。駆除後，PC を G さんに返却した。
- G さんに，マルウェア X の感染の原因と考えられるメールの削除を指示した。

図 5　調査結果と感染への対処

(5) 内部メールサーバの調査
・G さん宛てのメールを調査した。マルウェア X の感染の原因と考えられるメールは，5 月 2 日 20 時に届き，SMTP ウイルススキャンが行われたが，スキャン不能であった。
・5 月 4 日 10 時，V 社は，マルウェア X に対応したウイルス定義ファイルをリリースした。
・5 月 4 日 10 時 40 分，マルウェア X に対応したウイルス定義ファイルを，ダウンロードし，更新した。
(6) プロキシサーバの調査
・5 月 7 日 8 時 30 分～11 時，プロキシサーバにアクセスが集中し，応答が遅延していた。トラフィックの 90%が W 社の Web サーバへのアクセスであった。
・攻撃者の用意した C&C サーバの URL は，ベンダ提供ブラックリストに登録されていたが，マルウェア X 中の URL は登録されていなかった。
・マルウェア X 中の URL へのアクセス履歴はなかった。
(7) 従業員への周知
・5 月 7 日 17 時，社内通達として，業務サーバに次の事項を掲載した。
- マルウェア X の感染があったこと
- パスワード付きの添付ファイルを開く前に，最新のウイルス定義ファイルをダウンロードし，更新すること

図 5　調査結果と感染への対処（続き）

次は，E 主任と F さんが，中継サーバを経由するアクセスを防止する対策について検討した際の会話である。

E 主任：まず，当社のプロキシサーバと，マルウェア X の URL 中の中継サーバを経由するアクセスについて検討しましょう。

F さん：この中継サーバは，プロキシサーバの URL フィルタリング回避の手段として使われています。

E 主任：そのとおりですね。他のマルウェアが利用する可能性も排除するために，この中継サーバを経由する全てのアクセスを遮断することはできますか。

F さん：はい，③プロキシサーバのサーバ管理者登録ブラックリストに設定を追加することによって，遮断できます。

E 主任：今後，別の中継サーバを経由することも考えられます。プロキシサーバに設定を追加する業務手順を作成する必要がありますね。

F さん：はい，分かりました。

F さんは，プロキシサーバに設定を追加した。

E 主任は，図 5 の(4)では，G さん宛てのメールだけが対象であったので，追加の調査と対処が必要であると指摘した。指摘を受けた F さんは④メールについて追加

の調査と対処を行った。

さらに，E 主任は，パスワードを用いて暗号化されたファイルを添付したメールがインターネットから届いた場合に，メールの受信者に注意を喚起する必要があると指摘した。指摘を受け，F さんは，⑤図 3 中の結果の通知条件を変更した。

F さんは，HTTP ウイルススキャンでも，図 2 中の結果の通知条件の変更が必要であることに気付き，E 主任に報告の上，変更した。

E 主任と F さんは，ウイルス感染に関する調査結果と対処について D 部長に報告した。D 部長は，PC のウイルス定義ファイル更新遅延についての対策，及び管理用メールアドレス宛てに届くメールのウイルス対策についても検討するように指示した。

〔PC のウイルス定義ファイル更新遅延についての対策〕

E 主任と F さんが検討した結果，本社及び関西支社それぞれに，W 社のウイルス対策集中管理ソフトを導入したサーバ（以下，管理サーバという）を設置するとともに，PC のウイルス対策ソフトをウイルス対策集中管理ソフトに対応するものに入れ替えることにした。さらに，F さんがウイルス定義ファイルのダウンロード元の見直し案を作成することになった。ウイルス対策集中管理ソフトの機能概要を図 6 に，F さんが作成したウイルス定義ファイルのダウンロード元の見直し案を図 7 に示す。

(1) ウイルス定義ファイルダウンロード機能
・ウイルス定義ファイルを W 社の Web サーバから 1 時間ごとにダウンロードする。
(2) PC のウイルス対策管理機能
・PC からアップロードされる，ウイルス定義ファイルの更新時刻及びバージョン情報を保管する。
・PC からアップロードされるフルスキャン実行結果に関する情報を保管する。
・PC からアップロードされるウイルス感染情報を保管する。
・ウイルス定義ファイルをダウンロードして更新するように，PC に対して動作指示を送信する。
・フルスキャンを実行するように，PC に対して動作指示を送信する。
(3) 管理者向け機能
・管理者は，Web ブラウザを用いて上記(1)と(2)の情報を参照できる。
・管理者は，PC を指定して，ウイルス定義ファイルのダウンロード及び更新，並びにフルスキャン実行の動作指示ができる。

図 6　ウイルス対策集中管理ソフトの機能概要

(1) 本社の PC，業務サーバ及びファイルサーバ 1 のウイルス定義ファイルのダウンロード元を，本社の管理サーバとする。
(2) 関西支社の PC 及びファイルサーバ 2 のウイルス定義ファイルのダウンロード元を，関西支社の管理サーバとする。

図 7　ウイルス定義ファイルのダウンロード元の見直し案

E 主任と F さんは，ウイルス定義ファイル更新遅延についての対策案を，D 部長に提出した。D 部長は，対策案を承認した上で，ウイルス感染防止のためのウイルス対策集中管理ソフトの活用方法も考えるよう指示した。E 主任と F さんは，⑥D 部長の指示に従って活用方法を検討し，D 部長に報告した。D 部長は，活用方法も承認した。

〔管理用メールアドレス宛てに届くメールへのウイルス対策の強化〕

E 主任と F さんは，管理用メールアドレス宛てに届くメールへのウイルス対策の強化について検討した。

運用グループ用メールアドレス宛てに届く配送不能通知メールは，メールヘッダを確認すれば十分であり，添付ファイルを開く必要がない。一方，採用問合せ用メールアドレス宛て及び広報問合せ用メールアドレス宛てに届いたメールに添付ファイルがあった場合，その添付ファイルを開かざるを得ない。しかし，開くと，ウイルスに感染するおそれがある。

そこで，Java サーブレットを利用した問合せ用の Web フォームを公開 Web サーバに導入することにした。Web フォームには，ファイルのアップロード機能をもたせない。問合せ内容及び問合せ者の連絡用メールアドレスを入力してもらうと，受付通知メールを連絡用メールアドレス宛てに送信する。さらに，採用問合せ用メールアドレス宛て又は広報問合せ用メールアドレス宛てにも送信する。

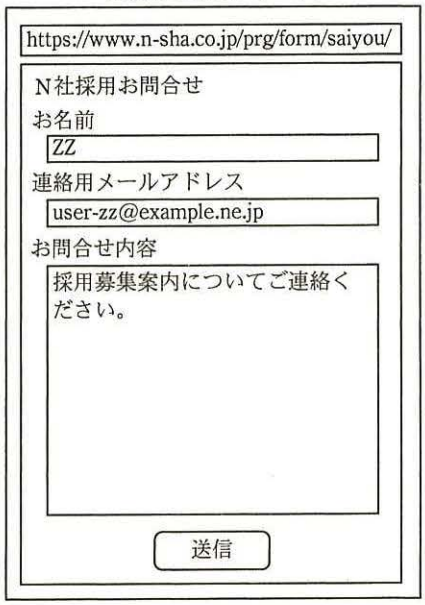
Web フォームの導入後は，採用問合せ用メールアドレス及び広報問合せ用メールアドレスを社外からは利用できないようにする。

〔Web フォームについての検討〕

Web フォームの設計は F さんが行い，レビューは，Web アプリケーションソフトウェアの設計に詳しい東ソリ本部の H さんに依頼することになった。

F さんは，採用問合せ用 Web フォームの動作概要を作成し，H さんとレビューを行った。F さんが作成した動作概要のうち，入力中の Web フォーム及び連絡用メールアドレス宛ての受付通知メールを，図 8 に示す。

入力中のWebフォーム



連絡用メールアドレス宛ての受付通知メール

```
 1  Date: Mon, 23 Jun 2014 15:00:18 +0900 (JST)
 2  From: saiyou@n-sha.co.jp
 3  Subject: Auto-Reply from N-SHA SAIYOU Group
 4  To: user-zz@example.ne.jp
 5  Message-ID: <20140623150018987654@n-sha.co.jp>
 6  MIME-Version: 1.0
 7  Content-Type: text/plain; charset=ISO-2022-JP
 8  Content-Transfer-Encoding: 7bit
 9
10  本メールにお心当たりのない場合は，削除してください。
11  このメールはシステムから自動送信されています。
12  返信はできません。
13
14  お問合せ，ありがとうございました。
15  問合せ受付について連絡します。
16
17  受付番号            : S-20140623-0015
18  お名前              : ZZ　様
19  連絡用メールアドレス : user-zz@example.ne.jp
20  お問合せ内容        :
21  採用募集案内についてご連絡ください。
```

注記 1　行番号は，メールには含まれない。
注記 2　1 行目から 8 行目は，メールヘッダである。

図 8　入力中の Web フォーム及び連絡用メールアドレス宛ての受付通知メール

H さんは，⑦採用問合せ用 Web フォームを悪用されるおそれがあるので，少なくとも図 8 の受付通知メールを，1～17 行目だけにすべきと指摘した。さらに，細工した連絡用メールアドレスを入力された場合の対策も必要であることを指摘した。

F さんと H さんは，レビューを続けた。次は，採用グループのメンバのメールアドレス宛てメールについての会話である。

H さん：まず，メールの本文について検討しましょう。アクセス者が，お問合せ内容として図 9 のとおりに入力したら，どうなりますか。

```
次の URL から私の履歴書をダウンロードしてください。
http://www.example.ne.jp/~kojin/rirekisho.pdf
```

図 9　H さんが示した入力内容

Fさん：入力したとおりに，メールの本文が作成されます。

Hさん：当社で使用しているメールソフトでは，“http://”と“https://”で始まる文字列だけは，行頭であっても，行中であっても，クリック可能なURLとして表示されます。もし，ウイルスをダウンロードさせるURLだったら，ワンクリックで，ウイルスをダウンロードさせられてしまいます。文字列の加工処理が必要となりますね。

Fさん：メール送信プログラム中に，図10の処理を追加する案で対処します。

```
（省略）
  //大文字と小文字の区別をせずに“http://”，“https://”を削除する。
  String resultMailBody = mailBody.replaceAll("(?i)https?://","");
（省略）
```

注記1　replaceAllは，第1引数に指定された正規表現にマッチする全ての文字列を，第2引数に指定された文字列に置換するメソッドである。

注記2　“(?i)”は，以降の正規表現を大文字と小文字の区別をせずにマッチさせるための正規表現である。

注記3　“https?”は，“http”と“https”にマッチする正規表現である。

図10　Fさんが作成した処理追加案

Hさん：図10は，対処として不完全です。例えば，図10の処理では，図11に示す文字列を入力すると，クリック可能なURLとして表示されてしまいます。

```
f ://www.example.ne.jp/~kojin/rirekisho.pdf
```

図11　Hさんが示した入力文字列

Fさん：なるほど，そのとおりですね。別の方法で対処します。

Hさんの指摘を受け，Fさんは，図8を含めて動作概要を修正した。

Fさんと Hさんは，さらに，広報問合せ用 Web フォームについてのレビューも行い，採用問合せ用 Web フォームと併せて，Web フォーム移行案としてまとめた。E主任の確認後，Fさんは，Web フォーム導入案をD部長に提出した。

D部長は，Web フォーム導入案を承認した。D部長は，管理サーバ導入に伴う情報システム予算の見直しを情報システム担当役員に説明し，承認を得た。

E主任と Fさんは，管理サーバの導入案と Web フォーム導入案の実装を開始した。

設問1　〔情報システムの構成〕について，(1)～(3)に答えよ。

(1)　表2中の［　a　］に入れる適切な字句を，英字8字以内で答えよ。

(2)　表2中の［　b　］，［　c　］に入れる適切な字句を，それぞれ10字以内で答えよ。

(3)　表2中の［　d　］に入れる適切なドメイン名を答えよ。

設問2　図3中の［　e　］に入れる内容を15字以内で答えよ。

設問3　本文中の下線①について，設定内容を45字以内で具体的に述べよ。

設問4　〔休み明けのPCのウイルス感染〕について，(1)～(4)に答えよ。

(1)　図5中の下線②について，改善されたN社の環境を活用して実施した内容を45字以内で具体的に述べよ。

(2)　本文中の下線③について，追加する設定の内容を30字以内で具体的に述べよ。

(3)　本文中の下線④について，調査した内容と対処した内容を併せて55字以内で述べよ。

(4)　本文中の下線⑤について，変更した内容を25字以内で述べよ。

設問5　本文中の下線⑥について，E主任とFさんが検討した活用方法を二つ挙げ，それぞれ50字以内で述べよ。

設問6　〔Webフォームについての検討〕について，(1)，(2)に答えよ。

(1)　本文中の下線⑦について，連絡用メールアドレスとお問合せ内容に何を入力すれば悪用することができるか。それぞれ20字以内で答えよ。

(2)　図11中の［　f　］に入れる適切な文字列を一つ挙げ，英字及び記号15字以内で答えよ。

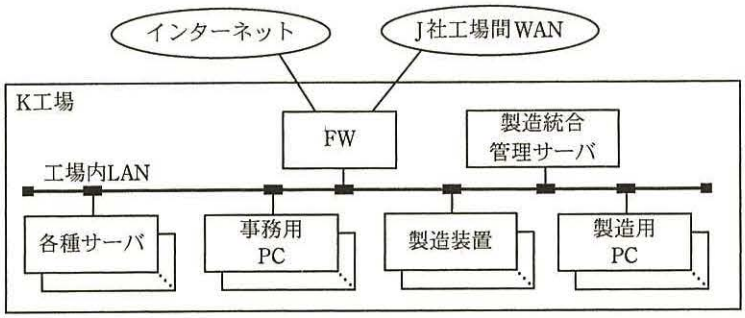
〔 メ モ 用 紙 〕

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，脆弱(ぜい)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。

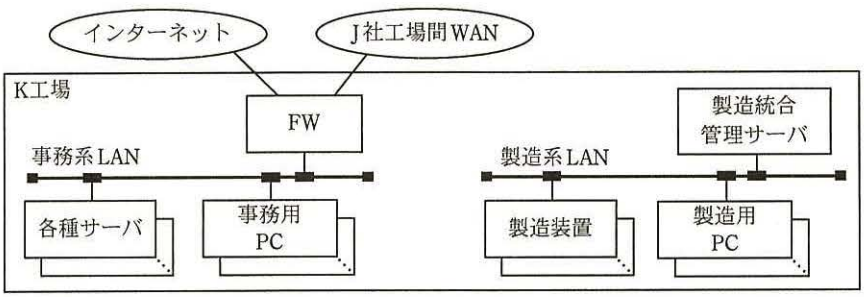
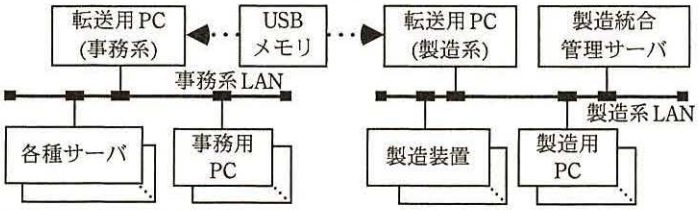
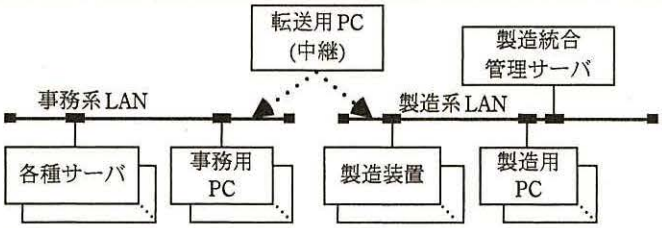


図２　工場内 LAN の構成見直し案

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。

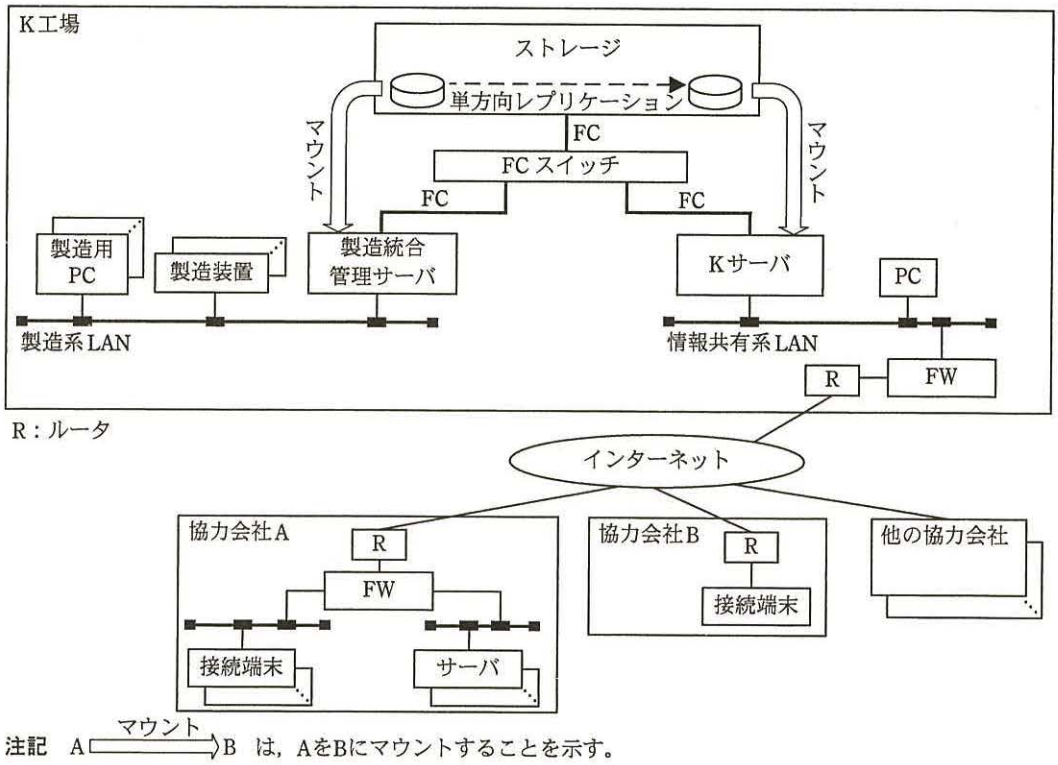


図４　Ｋサーバ及び関連機器の構成

(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。

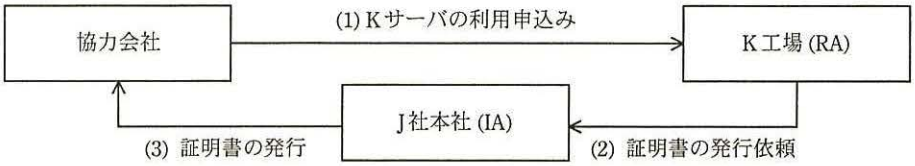
(2)　クライアント証明書による端末認証の採用

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。

6. 退室可能時間に途中で退室する場合には，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	15:10 ～ 16:20

7. **問題に関する質問にはお答えできません。**文意どおり解釈してください。
8. 問題冊子の余白などは，適宜利用して構いません。
9. 試験時間中，机上に置けるものは，次のものに限ります。
   なお，会場での貸出しは行っていません。
   受験票，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬
   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
12. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。

午